

Master's Thesis



Czech  
Technical  
University  
in Prague

**F3**

Faculty of Electrical Engineering  
The Department of Telecommunication Engineering

# Security and Authorization Management in modern telecommunication systems

**Bc. Vanja Neretljak**

May 2018

Supervisor: Ing. Tomáš Vaněk Ph.D.



## Acknowledgement / Declaration

First I would like to thank my thesis advisor Ing. Tomáš Vaněk Ph.D. from the Faculty of Electrical Engineering at Czech Technical University. The door to Ing. Vaněk office was always opened whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this thesis to be my own work, but steered me in the right direction whenever he thought I needed it. I must express my very profound gratitude to my parents and to my friends Ing. Ivan Golubović and Dejan Nedić for providing me with unfailing support throughout my years of study and through the process of researching and writing this thesis. This project would not have been made without them.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. V Praze dne 24.5.2018



## I. Personal and study details

Student's name: **Neretljak Vanja** Personal ID number: **420373**  
Faculty / Institute: **Faculty of Electrical Engineering**  
Department / Institute: **Department of Telecommunications Engineering**  
Study program: **Electronics and Communications**  
Branch of study: **Communication Systems and Networks**

## II. Master's thesis details

Master's thesis title in English:

**Security and Authorization Management in modern telecommunication systems**

Master's thesis title in Czech:

**Správa autentizace a autorizace uživatelů v moderních telekomunikačních systémech**

Guidelines:

Provide a brief description of SAML and LDAP protocols and their usage in telecommunications networks. Focus on 4G / 5G and NGN networks.

Compare their advantages and disadvantages over other currently used authentication mechanisms in telecommunications networks. Describe their usage in relation to the user management in EMS / NMS (Element Management System / Network Management System). Design, program and verify possibility of integration of Active Directory SSO (Single Sign-On) using SAML into web-based applications for MEDIO IN/OCS configuration and management .

Bibliography / sources:

- [1] RFC 7522, dostupné na: <https://tools.ietf.org/html/rfc7522> [on-line]
- [2] RFC 4511, dostupné na: <https://tools.ietf.org/html/rfc4511> [on-line]
- [3] RFC 4512, dostupné na: <https://tools.ietf.org/html/rfc4512> [on-line]
- [4] RFC 4519, dostupné na: <https://tools.ietf.org/html/rfc4519> [on-line]

Name and workplace of master's thesis supervisor:

**Ing. Tomáš Vaněk, Ph.D., Department of Telecommunications Engineering, FEE**

Name and workplace of second master's thesis supervisor or consultant:

Date of master's thesis assignment: **04.01.2018** Deadline for master's thesis submission: **25.05.2018**

Assignment valid until: **30.09.2019**

Ing. Tomáš Vaněk, Ph.D.  
Supervisor's signature

Head of department's signature

prof. Ing. Pavel Ripka, CSc.  
Dean's signature

## III. Assignment receipt

The student acknowledges that the master's thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the master's thesis, the author must state the names of consultants and include a list of references.

\_\_\_\_\_  
Date of assignment receipt

\_\_\_\_\_  
Student's signature

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Neretljak** Jméno: **Vanja** Osobní číslo: **420373**  
Fakulta/ústav: **Fakulta elektrotechnická**  
Zadávající katedra/ústav: **Katedra telekomunikační techniky**  
Studijní program: **Elektronika a komunikace**  
Studijní obor: **Komunikační systémy a sítě**

## II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

**Správa autentizace a autorizace uživatelů v moderních telekomunikačních systémech**

Název diplomové práce anglicky:

**Security and Authorization Management in modern telecommunication systems**

Pokyny pro vypracování:

Stručně a přehledně popište protokoly SAML a LDAP a jejich využití v telekomunikačních sítích. Zaměřte se na 4G/5G a NGN telekomunikační síť.

Porovnejte jejich výhody a nevýhody vůči jiným, v současnosti používaným autentizačním mechanismům v telekomunikačních sítích. Popište jejich využití v návaznosti na User Management v EMS /NMS (Element Management System/Network Management System). Navrhněte, zrealizujte a prakticky ověřte možnost integrace Active Directory SSO (Single Sign-On) pomocí SAML do webových aplikací pro konfiguraci a správu systému MEDIO IN/OCS.

Seznam doporučené literatury:

- [1] RFC 7522, dostupné na: <https://tools.ietf.org/html/rfc7522> [on-line]
- [2] RFC 4511, dostupné na: <https://tools.ietf.org/html/rfc4511> [on-line]
- [3] RFC 4512, dostupné na: <https://tools.ietf.org/html/rfc4512> [on-line]
- [4] RFC 4519, dostupné na: <https://tools.ietf.org/html/rfc4519> [on-line]

Jméno a pracoviště vedoucí(ho) diplomové práce:

**Ing. Tomáš Vaněk, Ph.D., katedra telekomunikační techniky FEL**

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **04.01.2018**

Termín odevzdání diplomové práce: **25.05.2018**

Platnost zadání diplomové práce: **30.09.2019**

Ing. Tomáš Vaněk, Ph.D.  
podpis vedoucí(ho) práce

podpis vedoucí(ho) ústavu/katedry

prof. Ing. Pavel Ripka, CSc.  
podpis děkana(ky)

## III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

\_\_\_\_\_  
Datum převzetí zadání

\_\_\_\_\_  
Podpis studenta

## Abstrakt / Abstract

Proces autentifikace a autorizace využívající Microsoft Windows Active Directory a moderní telekomunikační systém byl popsán v diplomové práci. Bezpečnost dat a informací je v 21. století jeden z hlavních problémů v telekomunikačních sítích. Tento projekt byl inspirován několikaletými zkušenosti v testovacím oddělení ve společnosti NVision, a.s. Použití Active Directory pro autentifikaci a autorizaci umožňuje urychlit veškerou práci na modulech Service Control Points (SCP). Použití protokolu LDAP přispívá k zabezpečenému procesu ověřování a autorizaci uživatelských práv. Konečným výsledkem projektu je funkční autentifikační a autorizační systém schopen implementace v moderní telekomunikační síti.

**Klíčová slova:** Autentizace, Autorizace, Active Directory, LDAP

**Překlad titulu:** Správa autentizace a autorizace uživatelů v moderních telekomunikačních systémech

Process of the authentication and authorization using Microsoft Windows Active Directory and modern telecommunication system, was described in this thesis. Security of data and information is, in 21st Century, one of the leading problem in telecommunication network. This project was inspired by few years work time spend on using the system for testing purposes at NVision, a.s. company. Using Active Directory for authentication and authorization process enabled all work on Service Control Points (SCPs) modules much faster. Usage of Lightweight Directory Access Protocol (LDAP) protocol assists in secure process of authentication and authorization of user rights. The final result of the project is a functional authentication and authorization system that can be implemented in modern telecommunication network.

**Keywords:** Authentication, Authorization, Active Directory, LDAP

# Contents /

<b>1 Introduction</b> .....	1
<b>2 Mobile network generations</b> .....	3
2.1 LTE and LTE-Advanced .....	3
2.1.1 Network architecture .....	4
2.1.2 Security process in LTE ...	6
2.2 5G Network .....	7
2.2.1 5G Architecture .....	8
2.2.2 Security and evaluation of differences between 5G and 4G .....	10
2.3 Next Generation Network .....	11
2.3.1 NGN Architecture .....	13
2.3.2 NGN Management .....	14
<b>3 Security mechanisms and Single Sign-On</b> .....	15
3.1 Security procedures .....	15
3.1.1 Authentication .....	15
3.1.2 Data confidentiality .....	16
3.1.3 Non-repudiation .....	16
3.1.4 Data integrity .....	16
3.1.5 Authorization .....	16
3.1.6 Resource availability .....	16
3.2 Single Sign-On (SSO) .....	16
3.2.1 Advantages and disadvantages of SSO .....	17
3.2.2 Protocols used in SSO system .....	17
3.2.3 Kerberos .....	18
<b>4 Lightweight Directory Access Protocol - LDAP</b> .....	20
4.1 Introduction to LDAP .....	20
4.1.1 Directories and LDAP ...	20
4.1.2 Distinguish Names - DN .	22
<b>5 Security Assertion Markup Language - SAML</b> .....	23
5.1 SAML Overview .....	23
<b>6 MEDIO IN/SCP</b> .....	26
6.1 General description of MEDIO IN/SCP platform .....	26
6.2 Architectural plan of MEDIO IN/OCS together with SCP modules .....	27
6.2.1 List of SCP modules: ....	27
6.2.2 OMM module .....	28
<b>7 Solution plan</b> .....	30
7.1 Architectural solution .....	30
7.2 Process solution .....	31
7.3 Active Directory structure .....	32
7.3.1 Active Directory Administrative Center .....	32
7.3.2 Active Directory domain controllers .....	33
7.3.3 The Active Directory data store .....	33
7.3.4 Active Directory partitions .....	33
7.3.5 Active Directory trust relationships .....	33
<b>8 Implementation</b> .....	34
8.1 Project realization .....	34
8.1.1 Virtual Box Machine ....	34
8.1.2 CentOS 7 .....	35
8.1.3 Windows Server 2012 R2 - Active Directory ....	37
8.1.4 LDAP protocol .....	38
8.1.5 Test Case - Nvision1 ....	40
8.1.6 Test Case - Nvision2 .....	42
<b>9 Conclusion</b> .....	44
9.1 Future work .....	44
<b>References</b> .....	45





# Chapter 1

## Introduction

Nowadays, security in mobile telecommunication systems represent one of the important fields in the world of new technologies. In this project I will describe characteristics of the last mobile telecommunication networks and together with their architecture we will try to explain role of security in them. Idea of this paper is to obtain as much information as we can about mobile networks such are 4G (LTE), 5G and NGN and according to their architecture to show implementation of the our own security system. Corresponding to research part we will decide how this security system will be accomplished and installed. Discussion about two different protocols (SAML and LDAP) will help us to realize practical part and together with SSO way of authorization they will be main characteristics of this work. We will discuss a use case that is of interest to many companies that are planning to centralize their authentication system.

Idea for this project came along with the information that many companies' struggles with the inside security system and with the complicated ways of authorization of their users. Especially in a world of web services users are forced to use multiple authentication credentials (usernames and passwords) for each application. Because of this they are faced with the use of same credentials for different services. This rise a potential risk of being unprotected and easy to hack. For better understanding security systems in mobile networks we decided to start this project with description of features and architecture of some of the last mobile networks. Chapter 2 examine three different types of mobile networks such are 4G (LTE), 5G and Next Generation Networks systems. Here we will outline basic information about how all networks work and what are differences in their architecture. We will focus on 3GPP statements connected to 5G networks and different services that can be provided by NGN.

In Chapter 3 will be examined some of the security mechanisms. Attention will be pay on services such are:

- Authentication
- Data confidentiality
- Non-repudiation
- Data integrity
- Authorization
- Resource availability

Also this chapter will cover description of the Single Sing On with its definition and different ways of using. SSO functionality and determination of the security of its protocols will be explained. We will outline advantages and disadvantages of using SSO and according to them we are going to choose best way for realization of our practical part.

Next part of this thesis will be focused on protocols that we already mentioned. Security Assertion Markup Language – SAML and Lightweight Directory Access Protocol – LDAP will be described. Their application together with their work flow will later be used in achieving our final goal.

Last, Chapter 6 will consider the plan of realization our own security system. We will consider previous research and according to it we will suggest the completion of the final practical product. Different parts and way of connection between them should help us later to make it functional as much as it is possible. In this part we will specify parts of Medio IN/OCS system that will be used in further work.

## Chapter 2

### Mobile network generations

In this Chapter we are going to focus our work on some of the last network generations. There is no need to go back to the mobile network beginning because our final work contemplate with the some of the newest network solutions. As we wrote on the beginning network generations that we are going to examine in this paper are 4G (LTE and LTE-Advanced), networks of 5G generation and as the last one Next Generation Networks – NGN. Because there are a lot of things to investigate according to the very complex solutions of these types of networks, we will concentrate our research on the basic information, architectural solution and usage of security systems in them.

#### 2.1 LTE and LTE-Advanced

In the time when already existing mobile networks technologies become systems that could no longer satisfy needs of huge number of users, network upgrade is necessary. The rapid increase in the use of the Internet to provide all kinds of services started at the same time as the 2G and 3G mobile systems were in extensive use. Next generation of mobile network should be able to support the same Internet Protocol (IP)-based services in a mobile world that common people use at home, using fixed broadband connection. Steps that led to the improvement of mobile network characteristics came in a shape of new technology that was named Long-Term Evolution or shorter LTE. Later this technology was improved to LTE Advanced and became fully part of the fourth network generation. There is need to highlight the fact that LTE and LTE-Advanced are the same technology, “Advanced” was added to interconnect LTE release 10 and ITU/IMT-Advanced. 3GPP (The Third Generation Partnership Project) established rules according to which new mobile technology (LTE) was set to the next level trough the achievement of better characteristics. These characteristics were in a form of use of higher bandwidths, better spectrum productivity, fully cooperation with other systems and of course wider coverage. LTE was introduced in Release-8 while later LTE-A was presented in Release-10. The LTE standards were fully completed at the end of 2008. [1]

Introducing LTE made expectations that a wide range of new mobile services will be available and that the old ones will be improved. Services as such were streaming video-on-demand, video conferencing, high quality VoIP, high-speed upload of multimedia content and others were planned to be improved. LTE stands for a new way of consuming wireless industry, targeting order-of-magnitude increase in bit rates. It aims to manage low-latency, packet-optimized radio access technology and on that way plans to advance spectrum flexibility. 3GPP made standardization for LTE to recognize the objectives of the International Mobile Telecommunications-Advanced (IMT-A) organization. To make these objectives operational, modern and sophisticated communication techniques such are MIMO (Multiple input multiple output) and OFDM (Orthogonal Frequency Division Multiplexing) were applied at the physical layer. OFDM-Access and single-carrier frequency division multiple access (SC-FDMA) helped in increasing spectral efficiency in both direction, in the downlink and uplink. Use of OFDM provides

a high degree of robustness against channel frequency selectivity. Even though problems with signal corruption due to a frequency-selective channel can be solved using equalization at the receiver side, OFDM became attractive because it is not so complex solution as the equalizer.

Multiple input/multiple output (MIMO) support expanded cell edge data rates and together with higher adaptive modulation and bandwidth selection upgraded mobility support. Important fact that made LTE different than previous network generations was that beyond the access layer it has been fully changed to an all-IP packet switched core network. Advanced packet core, improved base stations (evolved NodeB's) were introduced and joined to a high-speed data links. All these combinations helped LTE system to reduce control and user plane latency same as connection set-up and handover time. [2]

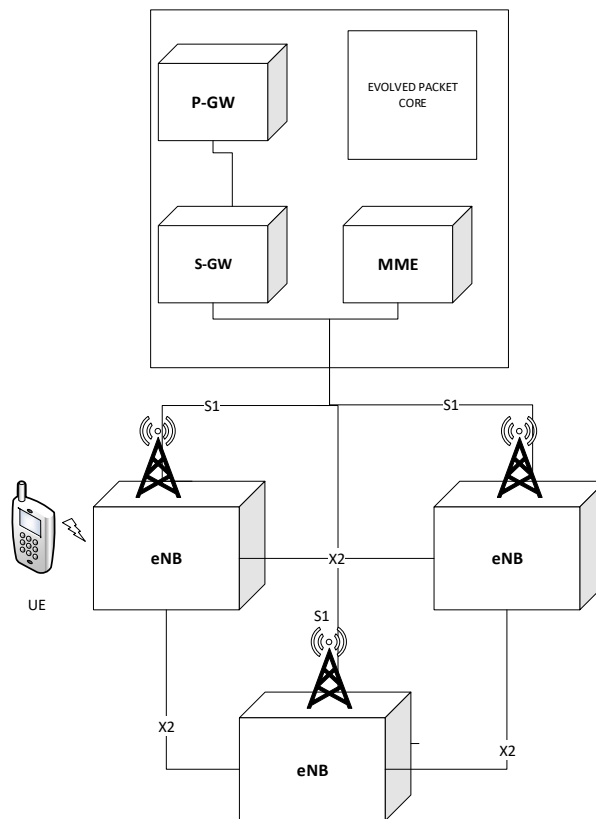
### ■ 2.1.1 Network architecture

Before introduction of LTE network architecture, in use were a hierarchical structure involving connection between the base stations and the central controller. This way of architectural solution required additional hops in both transmissions and hand off negotiation that led to a potential risk of delay. Because of the increase in global user number and with rise of online gaming and voice/video transmission through the internet the additional latency and delay in connection set up could decrease user-perceived quality of experience. To prevent situations that can lead to reduction of satisfaction in the set-up connection, LTE architecture involved the migration of local functions to eNBs and global functions to EPC. The eNBs play the important role in managing functions of radio network and medium access control. Many things have been transported to the eNBs such as negotiations, handoff requests and other local functions. Multiple eNBs may cooperate to determine the scheduling, transmission parameters, and transmit antenna weights for a particular UE. The plane architecture of LTE network is shown in Figure 2.1.

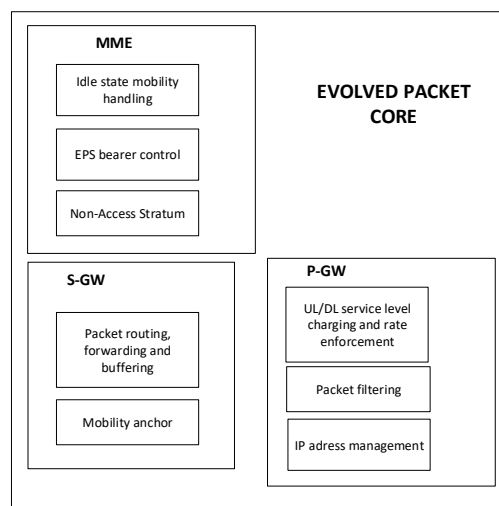
Connection between eNBs is made through X2 that present low-latency interfaces in an architectural configuration allowing improved and fast handover, including forwarding of line up data for unified user experience. Idea of this architectural solution tolerate, with direct connections between two cells, effective multi-point transmission and co-ordination management. By doing this the unload of the other network parts is also done. The evolved packet core or shorter EPC is in charge for all operations that are connected with external networks. Adding new layers in the network logic and division the various components made LTE network more useful in different ways. EPC is made by three different parts each of them has its own structure and role:

- Mobile Management Entity MME
- Packet Data Network Gateway
- Serving Gateway

MME has the main task in dealing with authentication, authorization and accounting functions. It solves problems such as connection and release of bearers to a terminal, management of IDLE to ACTIVE transitions. P-GW and S-GW modules are in charge of data packet forwarding, filtering and usage tracking. Serving Gateway represents a user-plane node that is in charge of connection the EPC and the LTE RAN. Packet Data Network Gateway interconnects the EPC to the internet. IP address allocation together with dealing with quality-of-service is operated by this part of EPC. These two parts of EPC acts as a mobility anchor for inter-eNB and inter-RAT handovers. Structure of EPC is depicted in Figure 2.2.



**Figure 2.1.** Basic structure of LTE cellular networks



**Figure 2.2.** Evolved Packet Core architecture

As already mentioned, with LTE and LTE-A there is huge progress in a downlink and uplink directions according to the data rate and spectral efficiency. In downlink direction, LTE is able to deliver 300 Mbps transmission data rate and 15 bps/Hz spectral

efficiency. This is accomplished by using OFDM as a modulation and 4x4 MIMO. Channel bandwidth is 20 MHz. Upload direction is provided by LTE with characteristic of 75 Mbps transmission data rate and 3.75 bps/Hz spectral efficiency. It is interesting that in uplink direction is used DFT-S-OFDM (Discrete Fourier Transform-Spread) or SC-FDMA (Single Carrier) with 20MHz channel bandwidth. In LTE-Advanced case situation is different in terms of transmission data rate and spectral efficiency. LTE-A is able to provide a 3 Gbps peak transmission data rate and 30 bps/Hz spectral efficiency in a download direction. It operates with Carrier Aggregation technique and 8x8 SM MIMO. Channel bandwidth is 100 MHz. In opposite direction transmission data rate is about 1.5 Gbps with 15 bps/HZ spectral efficiency. In use is same technique CA but with 4x4 MIMO. Radio-Frames represent structure of transmission in both directions. Each radio frame consists of 20 slots with duration of 0.5 ms, that makes 10 ms duration of one radio frame. There are 10 sub frames in one radio frame. Two dimension array called Physical Resource Grid is part of each slot. One dimension is matched to the time domain and the second one to the frequency domain. Structure of PRG is complicated and it will not be discussed in further text because there is no need for detailed explanation.

### ■ 2.1.2 Security process in LTE

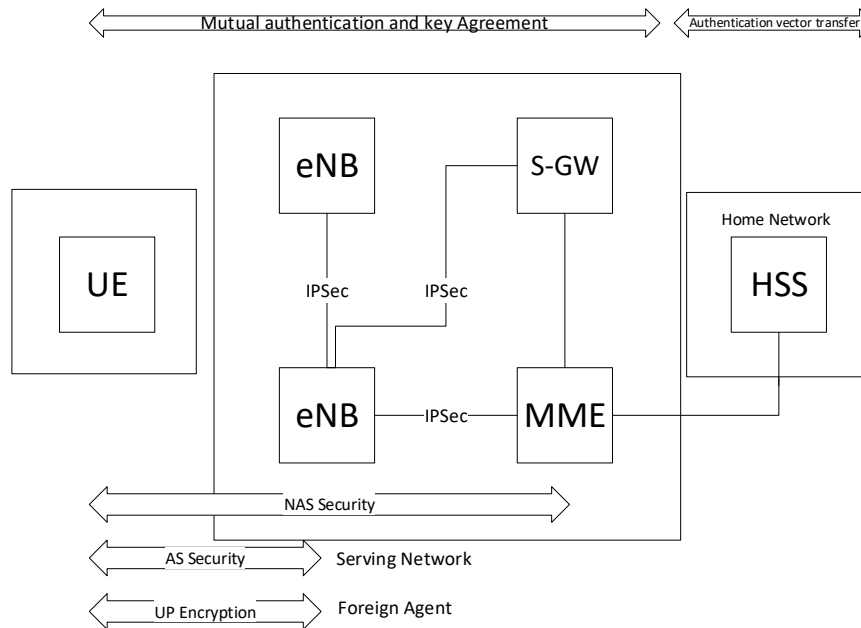
Since cellular networks have been upgraded through the time their security mechanisms also changed. There was a time where only one way of security authentication and key agreement was used. In case of 2G networks single authentication was applied. This meant that only network needed to authenticate the mobile phone. Later in 3G and 4G networks mutual authentication took place. Mutual authentication means that both sides, network and user equipment need to authenticate each other. According to 3GPP standardization LTE has to meet several specifications related to Radio Access Network (RAN). Evolved Packet Core plays an important role in terms of security in LTE network. Its design has been built up on previous systems GSM and 3G, but few additions were made. Evolved Packet System (EPS) can inter-work with legacy systems and this is made in backward-compatibility manner. Network entities, together with security protocols that are in charge for secure connection between these entities or sub-networks, are main features of EPS security architecture. The expanded architectural solution is shown in Figure 2.3.

Using Mobile Equipment authentication with serving network is done. A communication between EPS modules such as Evolved NodeB, Serving Gateway and Mobility Management Entity is secured by Ipsec. On the other hand data that are exchanged between the serving network and Mobile Equipment are assured by three different protocols:

- Access Stratum (AS)
- Non-Access Stratum (NAS)
- User Plane security (UP)

AS has responsibility to secure radio communication between User Equipment (UE) and the eNodeB. Non-Access Stratum ensures protected connection from the UE to the core network.

Security process in EPS is done once UE is identified. Next step is for MME to begin Authentication and Key Agreement (AKA) protocol. AKA protocol consists of three different steps/authentication procedures. First thing consider receiving a request from UE for authentication using MME. Here HSS generates EPS authentication vectors and sends them to MME. Next step is done by MME, choosing the one of the received



**Figure 2.3.** A High Level EPS Security Architecture

vectors for mutual authentication with UE, MME together with UE generate same authentication key using AKA set of rules. Last step is sharing new generated keys between the serving networks and the UE. This is done to make signaling and UP protection ongoing. EPS AKA achieves most of the security requirements of wireless network and successfully protects the communication interfaces against threats that were found in the preceding authentication and key agreement protocols of the access network. [3]

## 2.2 5G Network

As it has been outlined in previous section, 4G network systems were designed to fulfill the requirements of IMT-A using IP for all services. Even though this type of network was extreme progress in comparison to the previous, this was not enough for the telecommunication world. Due the rapid increase in the number of users who contribute to mobile broadband system and their demand for faster Internet access 4G network needed to be upgraded. Also technology progress in a form of new devices such are powerful smartphones and laptops claim advanced multimedia capabilities. Last researches showed that there was 92 percent growth in mobile broadband per year since 2006 to 2014.

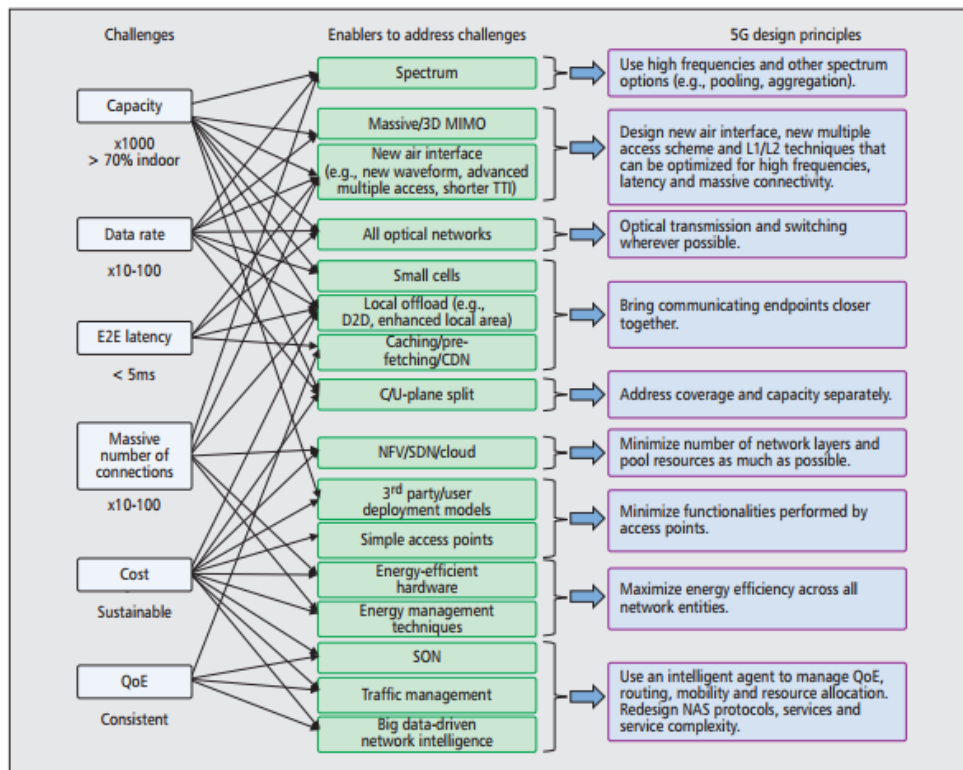
The most important thing in 5G networks is Flat IP network. This concept will make 5G acceptable for all types of technologies. Priority of the 5G is to fully respond on customer demands for real-time data applications delivery and secure connection. It uses packet switching and its continuous evolution provides improved performance and cost. There are six challenges that are set up in front of 5G network, that 4G was not able to process

- Higher capacity



- Higher data rate
- Lower End to End latency
- Massive device connection
- Reduced cost
- Consistent Quality of Experience provisioning

An overview of these challenges and its characteristics is shown in Figure 2.4



**Figure 2.4.** 5G challenges, potential enablers, and design principles

It can be noticed from the Figure 2.4 that the biggest challenge for 5G network is the physical lack of radio frequencies that are used for mobile communications. Frequency range that is in use for this purpose is between several hundred megahertz to several gigahertz and it has been already occupied as much as it is possible. Reduction of energy consumption is also one of the problems that 5G network took into consideration. This is step further in regard to previous network generation. This type of network with all characteristics represents challenge to mobile service providers also. There are a lot of projects that were and still are solving 5G demands and problems. Some of them are B4G project for wireless techniques or Siemens Networks description of radio access technology. A vision of 5G networks can be described in this way: “Networks will be the single, most indispensable element of future wireless connectivity, building an infrastructure of large-scale, complex and highly networked systems whose efficiency, sustainability and protection would require intelligent, interoperable and secure ICT solutions and novel business models.” [??] 2020 is a year when full 5G standardization is expected. Role of M2M communication is very important in a core of this network.

### ■ 2.2.1 5G Architecture



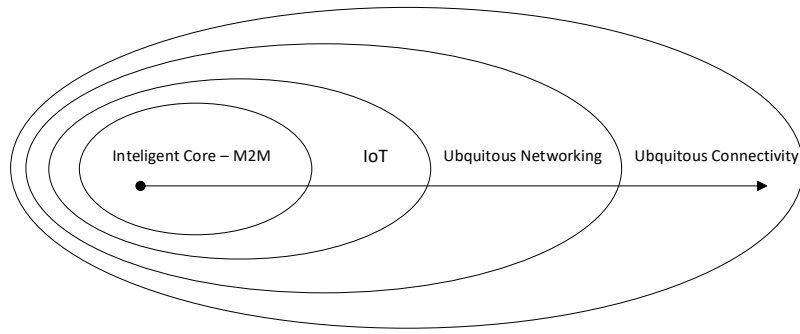


Figure 2.5. 5G system core idea

To understand the architecture of 5G it is important to comprehend the core idea. Three main aspects are significant for this network and they are shown in Figure 2.5

Intelligent core that is build up from M2M and IoT elements is a key for the ubiquitous networking and connectivity in 5G network. This type of core is able to respond to handling big data collected by M2M and IoT, their security and trust. Ubiquitous connectivity plays role in two different aspects. One is technical challenge related to necessary coverage range and second is enabling movement of application from device to device without problems. On the other hand enabling ubiquitous networking means as much as higher number of network connections. Their reliability and delivery services that need to be retained end-to-end.

Figure 2.6 shows general structure of 5G network architecture. [4]

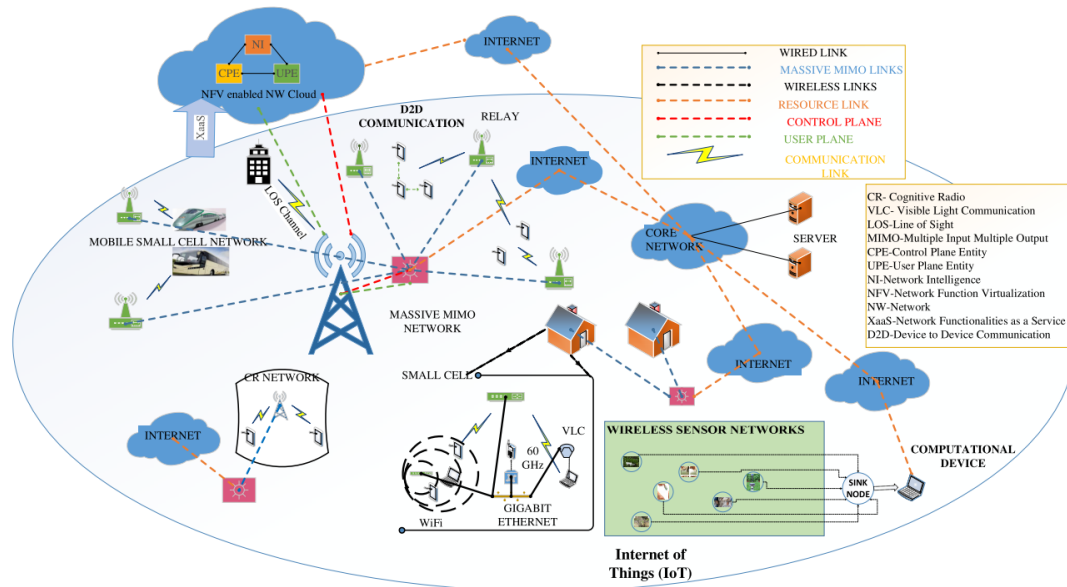


Figure 2.6. 5G system architecture

Progress that can be seen in 5G in regards to 4G network is usage of massive MIMO technology. It is upgraded version of the MIMO used in LTE and LTE-A. The difference that has been added in Massive MIMO technology is that this system contains few hundred antennas which are at the same time in one time, frequency slot serving tens of user terminals. The principle that is used in Massive MIMO is pretty much similar

to the previous version but only on a larger scale. There are few different things that make Massive MIMO dependent. Spatial multiplexing base station channel information are some of them. “In conventional MIMO systems, the base station sends the pilot waveforms to the terminals and based on these, the terminal estimate the channel, quantize it and feedback them to the base station.” [4]

The way how 5G network manages the control of the resources is important mechanism. There are two significant factors that put usage efficiency of resources to a higher level. Reuse and densification of the network are key aspects. These two aspects make 5G network efficient in utilization of limited resources and improvement in traffic capacity. In regards of exaltation of future cellular broadband systems there is constant need for more spectrum and wider bandwidths. To obtain this without problems, 5G uses two spectrum sharing techniques. They are categorized into two different solutions, distributed and centralized. Distributed solution characterize the solution where systems are coordinate between each other on an equal basis, while centralized solution presents solution where each system coordinates discretely with a central unit. In centralized solution systems do not directly interact. Characteristic of distributed spectrum sharing technique is that is useful in local framework while centralized technique is more effective in systems that have spectrum sharing on a higher level than the actual radio resources. From the Figure 2.5 it is noticeable the use of Device to Device Communication (D2D) system. This part of the network system can be divided into two levels, macro and device level. “The macro cell level comprises of the base station to device communications as in an orthodox cellular system. The device level comprises of device to device communications.” [4]

## ■ 2.2.2 Security and evaluation of differences between 5G and 4G

Because of 5G architectural complexity it is very important for security mechanisms to be flexible. This flexibility is consider in a way of different security layers together with different security procedures all integrated to one type of network. As an example it can be used user plane security that security can be provided by network or end-to-end security way. Which of these security procedures will be used depends on an applications and their demands. Also combination of different security mechanisms such are user plane security supported by network and user plane integrity protection are also available in 5G.

There are several different ways of security mechanisms in 5G. Since today there were different proposals how to build 5G security system. Some of them are connected to LTE security because till today this system appeared to be very reliable and safe. This system could be starting point on which 5G security will be built up. Of course it can come to the discrepancies with the 5G network architecture and this should be overcome in some way. Security procedure such is User Identity and Device Identity Confidentially was topic of previous systems where IMSI (International Mobile Subscriber Identity) was used for the permanent user identity. Under this procedure IMEI (International Mobile Equipment Identity) was used for the device identity. Another security mechanism that is called Mutual Authentication and Key Agreement and is in use in LTE networks could be part of 5G system also. AKA protocols are described in previous section. Security between Terminal and Network is done through signaling integrity procedure and is in charge of preventing impersonation of users and networks. As it ca been seen, 5G security system is basically upgrade of the already existing system in LTE networks together with some changes and additions.

It is of significant value for this thesis to understand differences between 5G and LTE networks in order to implement final work. Focus will be on technical characteristics and advantages/disadvantages of each network.

4G is synonymous with LTE technology and represents the development of the existing 3G wireless standard. On the other hand as it is described in previous sections of this thesis, LTE-Advanced represents the connection between 4G and 5G networks. This fact leads to the conclusion that LTE-A and 5G networks have several characteristics in common. In other words, 5G will improve some of the already existing features that are in use in LTE-A. Radio access network (RAN) below 6 GHz is used in 4G but it will be used in 5G networks only set to the frequencies between 6 GHz and 10 GHz. On earlier pages of this work it was talked about MIMO technology in both networks. It is important to write that 4G network today are in a rapid deployment, while 5G network still comprises projects and research works. 5G are being designed from their beginning to support machine type communication for Internet of Things (IoT) traffic, while 4G are able to support a modified MTCs. In term of offers, 5G will be able to deal with a plethora of connected devices and a huge number of different traffic. It will be first type of network that will use cloud RAN and virtual RAN to facilitate a more centralized networks.

More detailed differences between these two network generation can be seen on Figure 2.7:

Specifications	4G	5G
Full form	Fourth Generation	Fifth Generation
Data Bandwidth	2Mbps to 1Gbps	1Gbps and higher as per need
Frequency Band	2 to 8 GHz	3 to 300 GHz
Standards	AI access convergence including OFDMA, MC-CDMA, network-LMPS	CDMA and BDMA
Technologies	Unified IP, seamless integration of broadband LAN/WAN/PAN and WLAN	Unified IP, seamless integration of broadband LAN/WAN/PAN/WLAN and advanced technologies based on OFDM modulation used in 5G
Service	Dynamic information access, wearable devices, HD streaming, global roaming	Dynamic information access, wearable devices, HD streaming, any demand of users
Multiple Access	CDMA	CDMA, BDMA
Core network	All IP network	Flatter IP network, 5G network interfacing(5G-NI)
Handoff	Horizontal and vertical	Horizontal and vertical

**Figure 2.7.** List of technical differences between 4G and 5G networks [5]

## 2.3 Next Generation Network

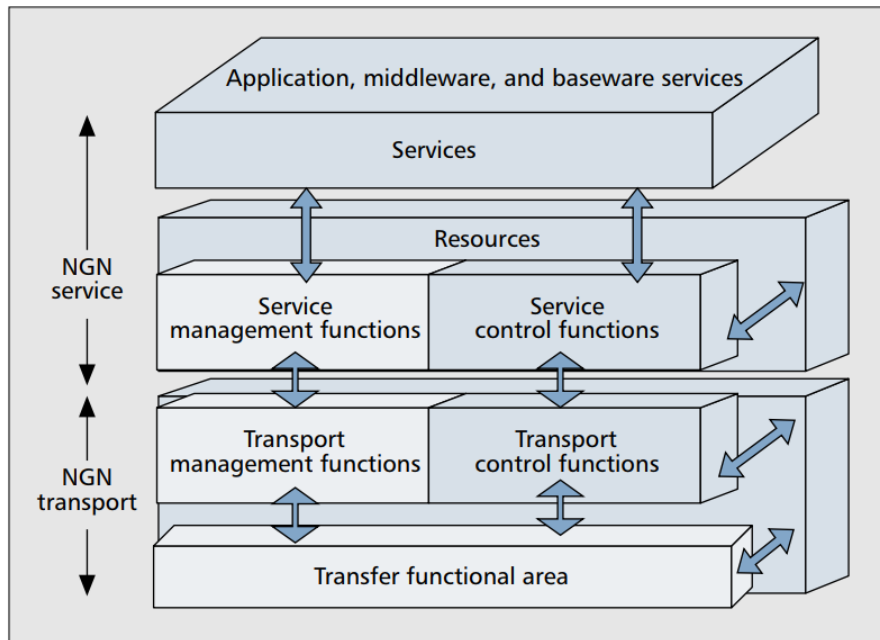
Main definition of NGN was created by International Telecommunication Union – Telecommunication Standardization (ITU-T) under the Y.2001 Recommendation, where beside definition are written necessary characteristics implemented in NGN. It defines NGN as: “A packet-based network able to provide telecommunication services and able to make use of multiple broadband QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies.” The Y.2011 Recommendation, additionally offers insight into the basic principles and qualities of NGN architecture and general framework.[6] Since the telecommunication market world is in fast change there was need for development of NGN. Two main features that were followed in this development were: [7]

- Development of mobile networks and exponential increase of the number of mobile users globally, so one may say that nowadays almost every human on the Earth has a mobile device (at least one)

- Development of the Internet as the only “survived” packet-switching technology worldwide and exponential increase of the number of Internet users, so one may expect that every human on Earth has or will have an access to the global Internet.

Important fact about NGN is that it supports generalized mobility. This will allow reliable and global provision of services to user. For better understanding purpose of NGN it is significant to determine the differences between NGN and traditional telecommunication services. Main transformation that happened in NGN is the shift from separate vertically integrated application-specific networks to a single network. This single network should be able of carrying and processing all needed services. As it can be noticed from NGN definition, transformation that happened is for example transition from circuit-switched infrastructure to a packet-switched for telephone service.

General functional model of NGN is shown on Figure 2.8. This model describes main features that are defined in Y.2001 Recommendation. Moreover, role of Y.2011 Recommendation is to provide core for developing functional models for NGN based services.



**Figure 2.8.** Functional model of NGN

According to fact that NGN is packet-based environment, this structure is expected to support a large number of new quality of service (QoS)- enabled services in every aspect of network. This means it should be able to maintain services involving an arbitrary combination of voice, video and data. Optimization for QoS – enabled services will allow broadband multimedia support. For NGN is essential to support changes that can be done by third-party service providers. This makes NGN control infrastructure and service architecture open and in that way more easily evolvable, with a much larger pool of technical staff who can quickly become productive in creating new features. Connection with customer premises equipment in NGN became in terms of service delivery more advanced. It means that NGN supports not only connection to various kinds of PCs but also to other wired and wireless devices and appliances ranging from screen phones to sophisticated multimedia workstations and media centers.

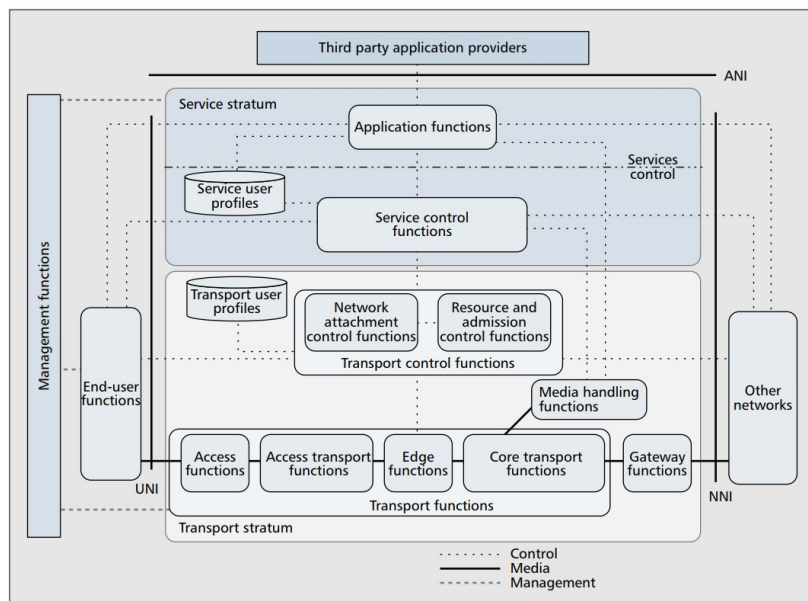
Protocols that are very important for NGN are Transmission Control Protocol - TCP and of course Internet Protocol- IP. Usage of this protocols make available transport of different types of services such are voice, data and other media through one network. Because of use of IP, sometimes NGN are described using this term.

In 2005 year, ITU-T promote the first release of documents that were taken as the first standards for developing NGN. Document under the name Release 1 specified all components for building NGN network. For example that document described functional architecture, NGN Framework and other key components. Group that was working on this release was named Focus Group on Next Generation Networks. Important fact was that this release was not fully implementable in that time, but it gave the fully described idea how to improve telecom networks.

The ITU is not only organization that published definitions for NGN. There is also definition provided by ETSI organization. Standards for NGN were made by TISPAN committee that today is not active anymore.

### 2.3.1 NGN Architecture

As the whole system is not so simple, its architecture also requires a lot of different components. Because today's architecture needs to support different types of multimedia services, such are video streaming and broadcasting, that architecture is composed of functional groups separated by well defined interfaces. Figure 2.9 shows the functional architecture of NGN that supports NGN described in ITU-T Rec.Y.2012.



**Figure 2.9.** NGN architectural plan

From the Figure 2.9 two main different parts in NGN architecture can be noticed. NGN service stratum is the part of network that gives user functions that are able to transfer service-related data to network-based service functions. Network-based part manages service resource and network services with main purpose of authorizing user applications and services. Services that are used in the NGN service stratum are voice, video, data etc. Important fact is that all of supported services in this part are related to services between peer entities, that explains that service stratum grants originating and terminating session between end peers.

The second part labeled as transport stratum has as main task to provide user functions that transfer data to the user. On the network's side transport stratum provides functions that control and manage transport resources for carrying the data. The main functional group that solve IP connectivity services to NGN users is transport stratum. It provides connection under the Transport control functions that include Network Attachment Control Functions (NACF) and Resource and Admission Control Functions (RACF). NACF part is used for terminals authentication inside the NGN. RACF is used when the authentication finish and terminals are able to communicate with NGN. RACF helps for example terminals to get desired QoS for communication.

There are several different principles according to which NGN architecture is build:

- Support for multiple access technologies
- Open service control
- Independent service provisioning
- Support for services in a converged network
- Enhanced security and protection
- Functional entity characteristics

Support for multiple access technologies means that NGN architecture supports different access technologies. Open service control describes NGN feature that represent control environment for example IMS, which is opened to different types of services. As the fact that transport and service stratum are divided in NGN service creation and delivery to end user is much faster and productive. Generalized services have easier access to NGN network because it provides merging of different access networks, and this is hidden under the support for services in a converged network. According to statement that NGN architecture provides open control of services there is a huge concern in terms of security. Last principle describes NGN as a network that is composed of many functional entities implemented in nodes in the network.

### ■ 2.3.2 NGN Management

Without proper ability to implement management side in the system, NGN does not have much reasons to be implemented. This means that management is the crucial part of the NGN because it brings ability to manage system services. This managing has to be secure and reliable as much as it can. Management functions have to operate with interaction between different entities such are FE and NE for example. All management functions are listed below:

- fault management;
- configuration management;
- accounting management (includes charging and billing functions);
- performance management;
- security management.

Much more information about management in NGN can be found in ITU-T M.3060.



## Chapter 3

### Security mechanisms and Single Sign-On

This Chapter will describe several security mechanisms together with Single Sign-On procedure, that are used in telecommunication systems of newer generations. In previous Chapter for each of mobile telecommunication network security system was explained, that is in use but in this part focus will be on security procedures that are connected with both telecommunication and IT systems. As it is was explained under the 5G and NGN networks connection with computer technology is in rapid growth. According to end goal of this thesis it is important to describe protocols that will be used for its realization.

#### 3.1 Security procedures

To describe the purpose of the security mechanisms it can be said that they present the set of rules that are applied in user activities in order to make security of information more improved. There are six basic security procedures that are applied today:

- Authentication
- Data confidentiality
- Non-repudiation
- Data integrity
- Authorization
- Resource availability

##### 3.1.1 Authentication

In network system, either it is spoken about telecommunication or IT system, authentication refers to verification of the identity of certain object in established system. There are two types of authentication: entity authentication and message origin authentication. For this thesis it is important to understand entity authentication type. This is because entity authentication is used in protocol securities. Its goal is the correctness of protocols, and not property of a single. The closest definition of entity authentication could be: “Entity authentication mechanisms allow the verification, of an entity’s claimed identity, by another entity. and, the authenticity of the entity can be ascertained only for the instance of the authentication exchange.” [8]A lack of precise definition is because nowadays is well known expansion of application areas in new environments that require more features to be incorporated in a protocol. To make it more effective and easier to use in everyday life process of authentication has to satisfy other security demands such are practicality, financial profitability, simplicity of servicing.

In order to be secure and correct, authentication procedure has to meet security definitions specified by its author. This includes security definitions such are security goals, syntactic specifications or implementations norms and an attacker model. All these requirements together give a definition of security analysis and can play a main role if it comes to attack attempts on the system.

### ■ 3.1.2 Data confidentiality

Confidentiality of data makes the information secure from the outside user. This means that no one who is not authorized to see information cannot control the data that are transferred. This is achieved mostly by using cryptographic way of sending information. Also the data should be stored on the receiver side in the same way, because it reduces the chance of manipulating them. Another way is also physical security of the communication line.

### ■ 3.1.3 Non-repudiation

To explain non-repudiation it is significant to define meaning of repudiation. This term can be explained as the rejection in having participated in all or part of an action by one of the entities involved. On the other hand, term non-repudiation is the power to protect against denial of the user or entity in an action of having participated. This procedure is typically useful in the transaction domain. It can protect system from potential attempts in cheating entities each other. [9]

### ■ 3.1.4 Data integrity

Description of data integrity demands exposure of any prohibited modification of data. This can be accomplished in several different ways, but usually it is done generating signatures or message authentication codes on the data for later verification.

### ■ 3.1.5 Authorization

An authorization represents the right granted to a user to exercise an action (e.g., read, write, create, delete, and execute) on certain objects. [10] This procedure often can be labeled with a term access control. Access control estimates the request to access resources and determines whether to permit or forbid them. Important issue connected to process of authorization is access control policy. On regulations of this policy authorization is based. For this thesis is essential to understand so called discretionary access control policy which enables authorization expressed in terms of the identity of the user. Since fact that users access is limited by proving their identity, process of authentication is needed.

### ■ 3.1.6 Resource availability

Availability of information refers to ensuring that authorized parties are able to access the information when needed. Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays. [11]

## ■ 3.2 Single Sign-On (SSO)

Single Sign-On represent the process of the authentication and authorization that enables user to preface his/her accreditation data only once so he/she can access to all allowed resources. After one authentication user can execute all tasks for which he/she has authorization. Authentication is based on marks. SSO is consider to be one of the best secure technologies that covers both of the security services. Today it is mostly spread and used for the Web security.

In another words, SSO is used for sharing authentication data. To formulate this simple as we can, we will use example of workers in one IT company. Employee has



to have access to different part of the company system, but not all of the employees has to have same access and same authorization rights. To create this, company has to implement authentication system that will manage rights that are assigned to each worker. If the employee wants to switch from one part of the system to another using same accreditation that he/she already used, there are few different ways for that:

- User name and password can be duplicated in data base for each application. So one application checks for itself whether is the password correct.
- Another way is to make sharing accreditation data between applications. This means that applications between themselves has to trust each other.

### ■ 3.2.1 Advantages and disadvantages of SSO

It is usual for the Single Sign-On module to be distinct in isolated part. From there we have the name “authentication at one place”. All application should trust SSO process and count on fact that it will be the one who will check user names and passwords. SSO system gives us several advantages:

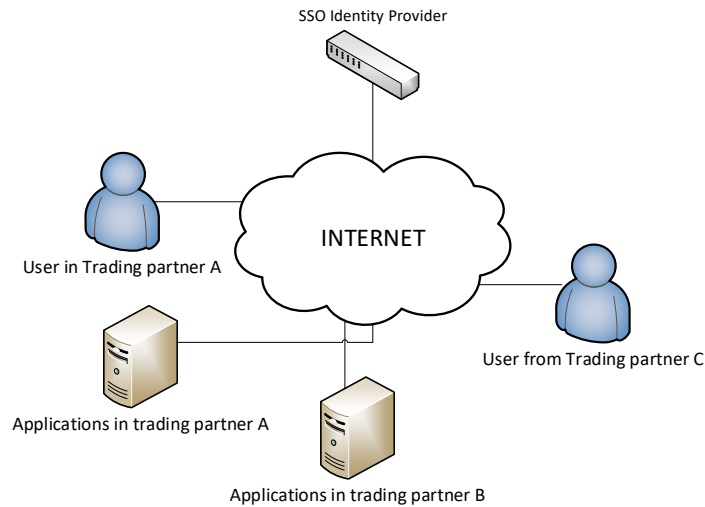
- Production of the user is greater than before. It support the fact that user needs to give his accreditation data only once at one place, enabling him to manage more than one part of the system.
- Authentication is based on a single database of security data.
- Fast and effective disabling and removing different types of accounts, weather they belongs to network or hardware.
- Improved scanning and tracking usage of different applications.
- Reduction of help costs. Here is meant reduction of costs that IT help desk needs to spend on a user

In order to discuss some problems that may occur using SSO it is important to accent that, list of disadvantages that are listed below, is not something that user should be afraid and they are not reasons to not used SSO for this thesis .

- Reason that makes user not to remember password also makes him lazy to use strong and complicated password. Password security will be taken to a question because of this. This situation would not be disadvantage for the system if administrator will make few rules that will ask user for more information or will require for example SMS Code activation.
- The way how SSO system works include third party in some authentication process. This will not be accepted by some companies and they will require from the administrator to implement in-house.
- In case that SSO goes wrong or gets attacked by someone from outside user will lose access to all platforms. So implementation of some backup is needed.
- If SSO is hacked for example trough one account, all other accounts are in danger.
- SSO should not be used for a multi-user computer. It is good for companies where multiple users can access to different platforms from a one computer.

### ■ 3.2.2 Protocols used in SSO system

Figure 3.1 shows how does Single Sing-on method looks like when it is implemented in some functional system:



**Figure 3.1.** Example of SSO usage

There are several different protocols that are being used for Single Sign-On method. OpenID, Kerberos and SAML are protocols that can be discussed in this thesis. OpenID protocol is very simple and enables clients to make their verification in process of accessing to some secure platforms. There are millions of users that are using this way of authentication in SSO system. Few steps that makes OpenID function-able are listed below:

- Relaying party defines login form to a user. User has to access URL that is actually his OpenID.
- Relaying party sends HTTP request to a OpenID. That request contain a documentation in which IdP endpoint is defined. Request also contain App ID that is identified by IdP and URL.
- User enters his accreditations in a form of a user name and password that are connected to IdP.
- Last step is that IdP sends back those information and redirects user to relay part together with authentication token that can be verified only by relay part.

### ■ 3.2.3 Kerberos

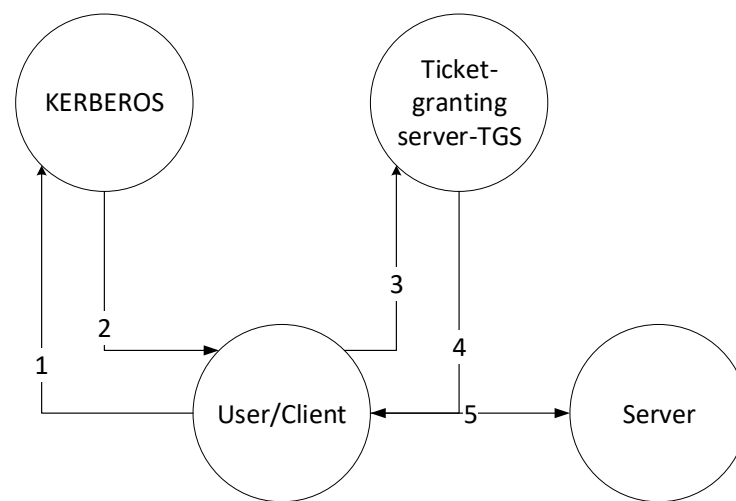
Authentication protocol that was developed under the MITs project Athena in the middle of 80s was named Kerberos. It stands for a distributed authentication service that enables a process, running on behalf of a user to prove its identity to a server or application server. This is done without sending data across the network and on that way data are protected from external exposure. Because of this, Kerberos is considered as a protocol that guarantees integrity and confidentiality for data exchanged between client and server.

Workflow of Kerberos is done without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will. [12]. It represents a trusted third-party authentication service and use conventional cryptography. Encryption in

this protocol is handled in the way that client has knowledge of an encryption key that is known by user but also authentication server. Process of authentication in this protocol is described in next steps: [12]

- A client sends a request to the authentication server (AS) requesting **credentials** for a given server.
- The AS responds with these credentials, encrypted in the client's key.
- The credentials consist of 1) a **ticket** for the server and 2) a temporary encryption key (often called a **session key**).
- The client transmits the ticket to the server
- The session key (now shared by the client and server) is used to authenticate the client, and may optionally be used to authenticate the server.

This process can be seen on Figure 3.2 :



**Figure 3.2.** Kerberos authentication protocol

- 1) Request for TGS ticket
- 2) Ticket for TGS
- 3) Request for Server ticket
- 4) Ticket for Server
- 5) Request for service

For secure usage of this protocol is important that it has to be installed on a carefully protected and physically secure machine. The best option is to be installed on a machine that is dedicated to run the authentication server and has limited number of users with access.

**Security Assertion Markup Language - SAML** protocol is described in details in **Chapter 5**.

## Chapter 4

# Lightweight Directory Access Protocol - LDAP

Chapter number 4 is consider to describe the fundamentals of access directories protocol named Lightweight Directory Access Protocol – LDAP. Beside its elements and architectural design it will provide information on its usage. In this Chapter focus will be on LDAP directories and their importance in this protocol.

### 4.1 Introduction to LDAP

LDAP represents one of several regulations for keeping and processing identification users data and their authentication on the server. Definition of this protocol describes it as a message protocol that is used by directory clients and directory servers. Its directories are hierarchical data bases and from the perspective of flexibility and simplicity of using, they have plenty advantages in regards to other traditional relations bases. Large number of completed software's solutions have integrated support for authentication and reading users information using LDAP.

LDAP was designed at the University of Michigan to adapt complex enterprise directory system to the Internet. Name of that directory system is X.500 system that is very complex and not so easy to describe. It is used for finding information about user's accounts from a server. Also using this Internet protocol in email world is very occasional. Organization that uses LDAP server in their companies have access to all contact information very easily.

LDAP was invented as a lightweight replacement for a DAP (Directory Access Protocol) and it simplifies some X.500 operations. It uses TCP/IP protocol stack rather than the OSI protocol stack. It is defined by a set of published Internet standards, known as Request For Comment (RFC) numbers, and published by Internet Engineering Task Force (IETF). Connection between LDAP and RFCs will be described in separate section. There are several different messages that are used in LDAP, such are bindRequest or searchRequest. This protocol stands for an open industry standard that is used for defining a standard method for accessing and updating information in a directory. It is important to mention that LDAP does not define the directory service itself, but only a communication protocol.

#### 4.1.1 Directories and LDAP

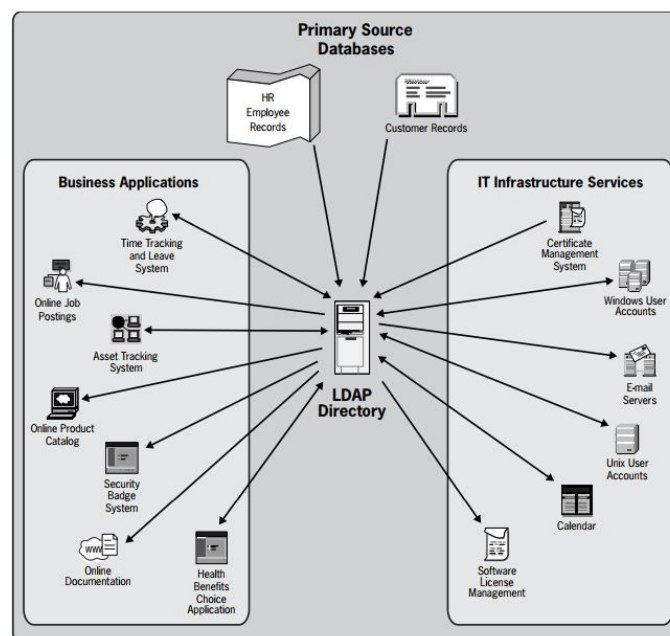
For better understanding of work principle of LDAP protocol, it is important to understand the meaning of a directories. Directories are designed to help in terms of better organization of different information. By this is meant not only an efficient way to find information but also to manage it. Directory can be used in many different ways, precisely it can be used for as much as there are different types of information. To describe it closer, there are three important parts of each directory: Structure, Content and Usefulness. Basic unit of the directory is entry. Characteristics of an entries are

that they contain a similar type of information. Composition of an entry is build up by collection of attributes or properties. Depending on how the directory is defined, entries can have a set of mandatory attributes as well as a set of optional attributes. [13] Last structural characteristics of a directory is that each attribute is composed of a pair of elements. In terms of content of a directory, it is considered to have entries that are static. This means that their update is infrequent in order to provide faster response. Directory can be compared to database, which contain information that are updatable often. Use of directories is well spread, but for this thesis their use in storage and managing of personal information can be useful. Because of their optimization to respond to queries about information that are constant through time, LDAP protocol uses them.

There are few different LDAP version that have been used in past, but today the best and the modernest one in way of specifications, is LDAP Version 3. According to its definitions LDAP does not define the directory service itself but it defines a communication protocol. In other words LDAP defines way of transport and format of message.

Authorization of rights that can be added to users in LDAP is very rare. Mostly this protocol enable users to read information but only few can make updates. Problem that often occurs here is that LDAP does not have such strong security or encryption. Because of that it is frequently interpreted by some of the encryption such is SSL connection to the LDAP server. Two characteristics that are defined by LDAP protocol are Permissions and Schema. Permission is the set of defined rules that allow access to LDAP data base selected number of users, and those rules are set by the administrators. Schema represents the description of a design and attributes of data in the server.

The idea of LDAP is required today much more then in the beginning. The main topic that lays under the idea of LDAP can be understood from words that Tim Howes said in one interview that having a single point from which you can control access has always been key. [14] Today the Internet resources that are used are so much more decentralized and together with huge number of different services make need for LDAP protocol larger. On Figure 4.1 is shown example of LDAP usage in company purposes:



**Figure 4.1.** Example of LDAP usage in company purposes

### 4.1.2 Distinguish Names - DN

LDAP entry structure is made up of a group of features that must have a distinctive identifier called a Distinguished Name (DN). Hierarchy in this system must be followed, because of that a DN has a unique name that identifies the entry in the system. As an example can be used, name of two people that present common names (cn) identifies different entries at the same level. It is important to understand that X.500 Directory has this DN as the main entries in the directory. Distinguished Names are encoded in ASN.1 in the X.500 Directory protocols. In the Lightweight Directory Access Protocol, a string representation of distinguished names is transferred. This specification defines the string format for representing names, which is designed to give a clean representation of commonly used distinguished names, while being able to represent any distinguished name.

A DN [15] is typically composed of an ordered set of attribute type or attribute value pairs. Most DNs are composed of pairs in the following order:

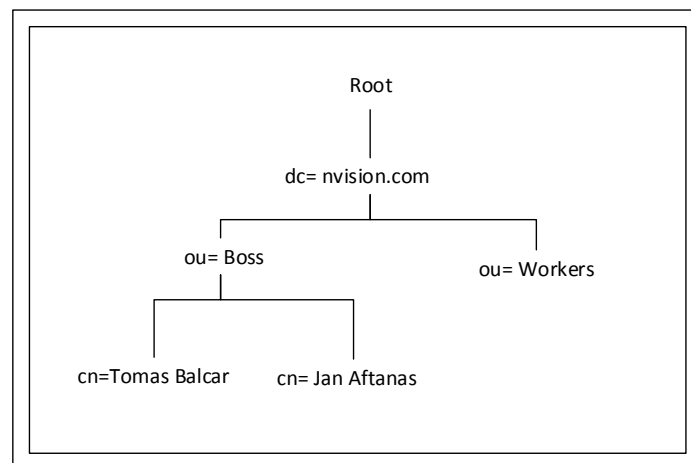
- Common name (cn)
- Organization (o) or organizational unit (ou)
- Country (c)

Example of DN that can be used is:

**cn = Tomas Balcar, ou = Boss, dc = nvision.com**

Where **cn = Tomas Balcar, ou = Boss** represents Relative Distinguished Name (RDN) to the root RDN **dc=nvision.com**

Figure 4.2 shows the structure of LDAP directory with distinguished names and relative distinguished names



**Figure 4.2.** Example of LDAP Directory Structure

## Chapter 5

# Security Assertion Markup Language - SAML

In this chapter focus will be on Security Assertion Markup Language or shorter SAML protocol. This protocol was created by OASIS Security Services Technical Committee and version that is spread the most in IT world is SAML 2.0. This protocol use XML-based data to construct trust and reliable authentication transfer. SAML provides user to exchange identity information through different application and services. The Security Assertion Markup Language (SAML) standard defines a framework for exchanging security information between online business partners.

### 5.1 SAML Overview

The way in which today access, to different modules or entities, works requires a multiple user-name and password input. The administration of these user-names and passwords demands very complicated work to be done. In IT or the Internet world each system requires registration of new user in order to access some service or application. There are exceptions, systems that allow client to use authorization trough already existing account, for example Facebook or Google. But this way of authorization is not reliable if it needs to be implemented internal, for example in a company. The best solution in this case could be use of SAML protocol.

Information that is transferred between entities by SAML protocol is the secure information expressed in the form of assertions about subjects, where subject is an entity that has an identity in some security domain. Subject that represents this entity can be human, but in most cases this subject represents company. SAML [16] assertions are made by system entity that is called asserting party or sometimes a SAML authority. On the other side there is entity called relying party and its main charge is to use received assertions. Interesting fact about these

assertions is that they can deliver information authentication acts performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources. Structure of assertions is based on XML format. There are three kinds of SAML assertion statements:

- Authentication statements describe a subject authentication event (e.g., when, by whom, via which authentication mechanism)
- Attribute statements provide details of the subject (e.g., the department in which the subject works)
- Authorization decision statements indicate whether the subject has permission to access a particular resource

It is important to point out that SAML provides protocol that enables users to request assertions from SAML authorities and get response from them. This protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport protocols; SAML currently defines one binding, to SOAP over HTTP.

There are few SAML actors that need to be defined:

- **Service provider:**  
Protected data, are stored on this server. This data can be in different forms and are accessed by user or by means of an API. This API is provided by the service provider.
- **Client:**  
Represents the entity that is requiring access to SP entity and to data in it. SAML 2.0 only supports the web browser SSO profile as a client, meaning, the client always connects to the service provider using a web browser as its User-Agent.
- **Identity provider:**  
This party checks the identity of clients and issues assertions to allow or deny access to protected resources.

As it is already mention above, SAML is XML framework, which means that XML documents are used for authentication of information. SAML is standard for SSO format. This characteristic gives SAML huge advantages in a way of using username and password to gain access. In fact, there is no need to type in credentials, passwords should be strong and there is no need to remember them. These elements make SAML very complicated SSO implementation. The standard that defines SAML requires request and response protocol used to make communication between different parties such are relaying party and asserting party. Examples of SAML protocols are:

- Authentication Request Protocol
- Single Logout Protocol
- Artifact Resolution Protocol
- Name Identifier Management Protocol

Each protocol has its own role and function. For example we can describe Authentication Request protocol as such protocol that defines how the service provider can request an assertion that contains authentication or attribute statements. Single Logout Protocol defines way of logging out of all service providers. Third protocol Artifact Resolution Protocol describes values such are initial value and request/response value are passed between the identity provider and the service provider. Last protocol that is on the list explains the method of adding, changing or deleting the value of the name identifier for the service provider. For better understanding how actually SAML works we can examine its work flow. Two processes that are included in this protocol are trust establishment and authentication flow. To show example procedure we can use:

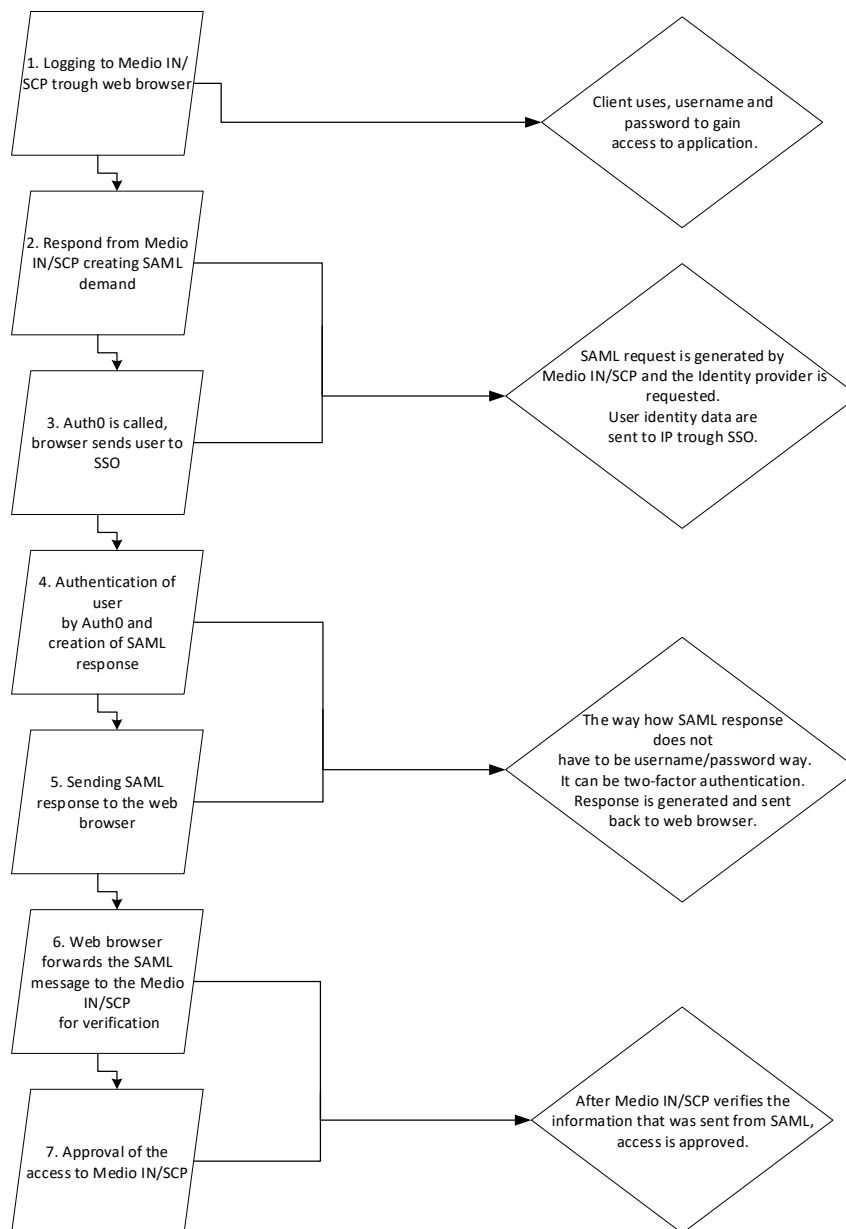
- Identity provider (IP) will be marked as Auth0
- Service provider is company portal termed Medio IN/SCP

Parameters that are very important in this protocol are listed below:

- **ID:** Identification number used for process
- **IssueInstant:** Gives correct time when it was generated
- **AssertionConsumerServiceURL:** Place where IP part sends the auth. token
- **Issuer:** The identity of SP
- **InResponseTo:** Identification number of SAML request that calls response
- **Recipient:** Address of the SP

Situation where user requires access to Medio IN/SCP trough SAML authentication process, starts with first step: trying to access Medio IN/SCP using web browser. The whole process can be seen on the flow graph 5.1:





**Figure 5.1.** SAML - Workflow diagram

Workflow on Figure 5.1 shows the imaginary way of authentication on MEDIO IN/SCP platform using SAML protocol. This system is described in detailed in next chapter, and because of its complexity and architecture, for this project will be used only a part of the whole system.

## Chapter 6

### MEDIO IN/SCP

Following Chapter will be consisted of detailed description of the system that will be used for implementation of the final work. As it was already mentioned in previous chapters this system is called Medio IN/SCP. MEDIO IN/OCS, which is online charging system by NVision Group, is a flagship product based on MEDIO IN/SCP platform and it fully uses platform with highly efficient and secure environment.

#### 6.1 General description of MEDIO IN/SCP platform

MEDIO IN/SCP is modern versatile communication platform with following features:

- High performance, low footprint
- High availability and fail over
- Support for all current signaling and charging protocols: SIGTRAN, SIP, Diameter
- Advanced monitoring and manageability features (alarm collections, performance measurement, state and configuration management)
- Easy integration with external systems

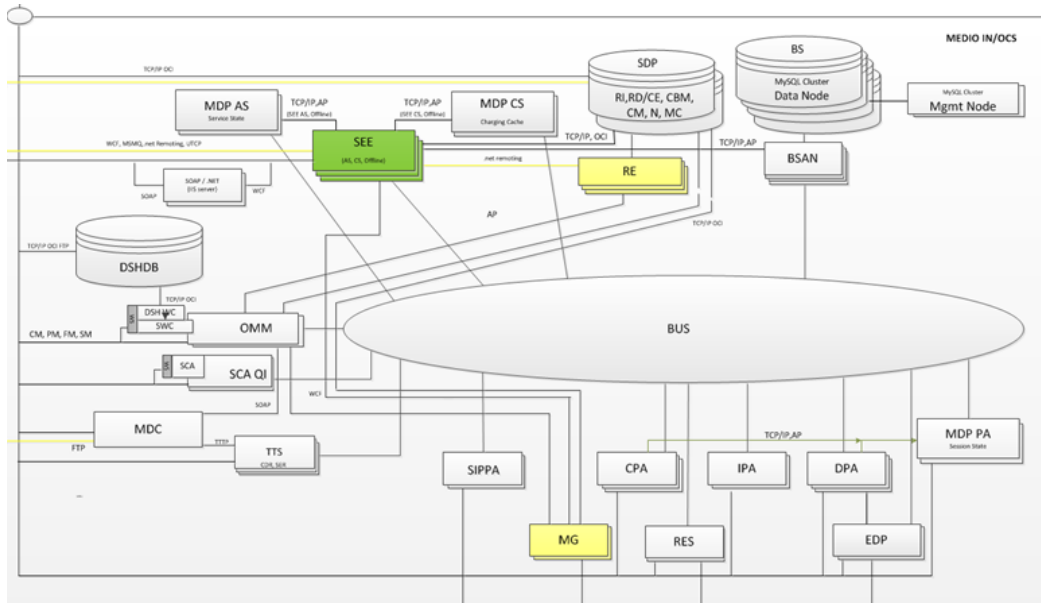
MEDIO IN/SCP enables operators to achieve considerable Capital Expenditure (CAPEX) and Operating Expenditure (OPEX) savings by shortening the time-to-market when making modifications to existing services, and reducing the time-to-market and the cost of introducing new services, as well as lowering overall operation expenses as a result of the unified customer centric architecture . MEDIO IN/SCP is a modular, component based system, with open interfaces. This enables it to easily integrate with other applications such as Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), NVision's own FORIS OSS or other vendor's billing solutions and service and content delivery systems or legacy software. It's possible to implement only certain modules of the system and integrate them with external applications.

The MEDIO IN/SCP platform can be scaled to satisfy the growing needs of the operator and preserve their investment. The system is fully scalable, from the smallest installation (1 000 000 active subscribers) up to the biggest one (6 000 000 active subscribers) in several steps. System capacity is measured in number of active subscribers. It's assumed that on average each active subscriber during busy hour generates load, described in Online traffic model. Subscribers are considered active during any given day when there was activity registered from their terminal device within time period of last 90 days. Date of last activity is stored for each subscriber and subscriber's account in SCP database.

System capacity is dimensioned so in addition to nominal projected capacity, there may be up to 50 percent of inactive subscribers provisioned in DB. For example, for maximum capacity of 6 000 000 active subscribers there may be up to 3 000 000 inactive subscribers, making it 9 000 000 subscribers in total. Greater number of inactive subscribers, while not immediately harmful to system stability, may lead to insufficient performance of SCP during high load periods, and therefore is not recommended by vendor.

## 6.2 Architectural plan of MEDIO IN/OCS together with SCP modules

The MEDIO IN/SCP platform is an open modular system comprised of a number of functional components:



**Figure 6.1.** MEDIO IN/OCS together with SCP modules

### 6.2.1 List of SCP modules:

- BS (Balance Storage) is a MySQL Cluster database keeping subscriber balances and providing overall Balance management functions
- BSAN (Balance Storage Application Node) is an interface module to access Balance management functions of BS
- BUS provides means for efficient internal communication between MEDIO IN/SCP modules
- CPA (CAMEL Protocol Adapter) allows deploying CAP and MAP protocols for integration with external Network Elements
- DPA (Diameter Protocol Adapter) allows deploying Diameter protocol for integration with external Network Elements
- IPA (ISUP Protocol Adapter) allows deploying ISUP protocol for integration with external Network Elements
- SIPPA (SIP Protocol Adapter) allows deploying SIP protocol for integration with IMS core
- EDP (Embedded Diameter Proxy) single point of contact for all Diameter signalling
- MDC (Mediation Device Cluster) collects CDR and SER files from TTS modules, stores and exports CDRs to OSS/BSS or other external systems
- MDP (Memory Data Provider) is used for fast access to session data. All information is stored in the RAM of module and only for duration of the charged session
- MG (Messaging Gateway) provides outgoing notification interfaces to SMSC, HLR or other external systems with support of notification scheduling, queuing and logging.

- OMM (Operation and Maintenance Module) serves for gathering of management data from the rest of platform modules and performing management operations on them
- RE (Rating Engine) is a module performing online rating of services
- RES (Router of External Signalling) routes the messages to or from the external network elements, enveloping SS7 and SIGTRAN messages for internal delivery
- SCA QI (Subscriber Care Application Query Interface) serves as translator from the JSON (Javascript Object Notation) used by the SCA web server where runs the SCA GUI to application protocol used by SEE.
- SDP (Service Data Point) is an Oracle DB used for storage of subscriber data, tariffs and product catalogue, resource inventory, configuration management information
- SEE (Service Execution Environment) allows implementing and deploying service scenarios and different API interface managers
- SIPPA (SIP Protocol Adapter) allows deploying SIP protocol for integration with external Network Elements
- SOAP Provider provides open interface to access MEDIO IN/OCS services through SOAP interface
- TTS (Tool Ticket Server) collects charging-related events and creates CDRs (Charging Data Record) and SERs (Service Event Record) based on collected events

### ■ 6.2.2 OMM module

For purpose of this thesis, module that will be used is called Operation and Maintenance Module – OMM. As it can be read from its definition it is used for gathering of management data from the rest of modules. Also it is used for performing management operations on those modules. In situation for this thesis, it will be used as a first point of communication with Element Management Service – EMS module. EMS module will be described in detail in next chapter. Here will be outlined few characteristics of OMM module.

Detailed description:

- OS: Linux Debian 7.0 (Wheezy)
- Configuration Management - CM
  - OMM stores the configuration files for BUS modules
  - OMM acts as a central point for controlling of MML commands and reports for all MEDIO IN/SCP modules. The operator communicates to OMM, which handles all MML commands.
  - OMM receives MML commands from Web Console and applies MML command transformation on it.
- Fault Management
  - OMM creates a common platform to perform OandM tasks in MEDIO IN/SCP and to create a standard interface(s) towards the management system (OM Tools, ZENOSS or 3rd party), as well as server side for OM agents at modules.
  - OMM receives SNMP traps from modules based on BUS technology
- Performance Management
  - OMM receives and stores notifications and result reports from BUS modules; it then forwards them to OMS

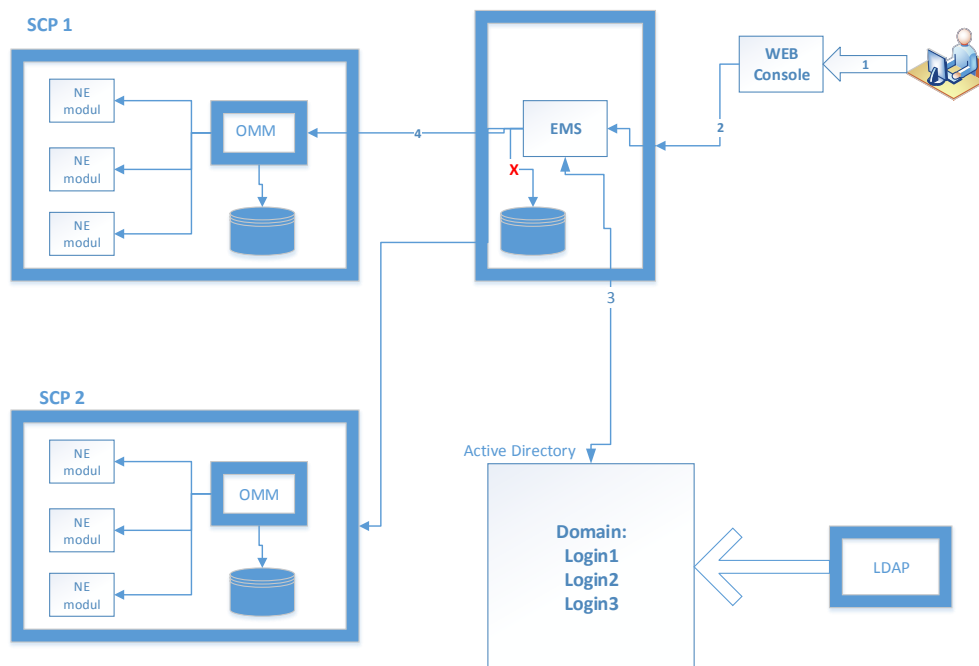
- OMM controls measurement jobs on request from external EMS/NMS (start, stop, suspend and so forth) and distributes necessary operations/parameters to OandM agents
- OMM collects measured data prepared by OandM agents
- OMM transforms measured data into xml files with naming conventions and structure defined by 3GPP. Files are stored at in folder hierarchy of server OMM runs on
- OMM, on behalf of operator of management system (ZENOSS or 3rd party), takes care of administration of measurement jobs for all modules based on BUS technology
- OMM distributes necessary operations/parameters to OandM agents
- OMM agents in modules based on BUS technology perform start, stop and suspend commands
- OMM serves as a Time server for all BUS modules (Time server runs on the hardware where simultaneously should run also OMM as a separate service not connected with OMM.)

# Chapter 7

## Solution plan

In this Chapter, the description of a solution plan, that will be used for this thesis, will be presented. Besides the organization plan, here the list of different modules and their basic characteristic will be explained. Also, this section will contain description of a work flow process together with implementation of previously described protocols. Each part of the system will be labeled and will have a detail description of its tasks.

### 7.1 Architectural solution

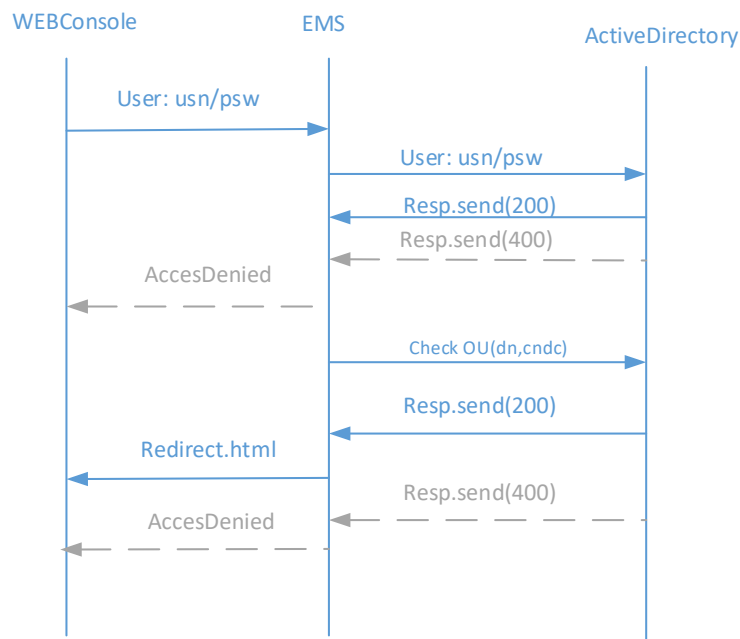


**Figure 7.1.** Architectual solution plan

Figure 7.1 shows the architectural solution plan of the main object of this thesis. As it can be seen there are few different modules. EMS module will be the center of the whole process. This module, in the work process will represent web application running on Linux OS, and it will work as a gateway to different Service Control Points – SCPs modules. Also EMS will have main responsibilities to communicate with Active Directory. Construction of Active Directory – AD will be explained in next section.

## 7.2 Process solution

Basic flowchart is planned to be as it is shown on Figure 7.2. The idea of this process is to bind Active Directory and all data to login (authentication and authorization) check. Main point is to make secure connection between EMS and Active Directory. Another important thing is to correctly develop login question that will be sent from the web to EMS. The design of the system requires connection between two different operating systems. EMS application will be made in some of the versions of Linux system, while Active Directory will be set up on Microsoft Windows system. Once connection is established and login information will be able to be sent to an Active Directory, authentication process can be done.



**Figure 7.2.** Idea of flowchart

Authentication process should be realized using LDAP or SAML protocol. One of these protocols will be able to deal with specific check and ability to give authorization to a user that is registered in Active Directory. Protocol has to be capable to make deep and fast search of user credentials. This should be enabled because structure of an Active Directory will contain different users with different authorization rights. Once user is found in Active Directory, response should be sent to EMS allowing redirection to an SCP part of the system. Different users' needs to have different access rights. From the process of authorization all other database that were before included in the process, will be omitted. One of the main point of this system is to make fast search, protected connection and accurate authorization method that will replace old database system by usage of Active Directory.

In case that process comes to a point where there is no registered user in Active Directory, access to the EMS has to be denied. This is also one of the reasons to make proper and fitting login method at the beginning of flowchart. Login method, first of all, needs to be easy to use for a client. Input parameters should not be long, complicated and to require additional information from a user. This method has to be reliable and also useful for the other, Active Directory, side. User has to be able very

easily to remember his credentials. Only if user's identification data matches to data that are implemented in Active Directory authentication process could be done in a positive way. Otherwise, access needs to be denied. On the other side if user wants to access parts of the system that he/she does not have right to, access needs to be denied. All authentication and authorization process should be complete by one of the already mentioned protocols.

## 7.3 Active Directory structure

Active Directory is well known as a service whose main purpose and goal is to automate network management of a user data, its security and distributed resources. Microsoft Windows considers Active Directory for a core component of the server infrastructure. Design of Active Directory enables a secure environment for managing, users, services and resources. This way the system that is in charge of centralized authentication and authorization processes it had been successfully created. Active Directory can be described as a phone book, containing data about people, their numbers, addresses and other private information. Considering this, it is a perfect solution for this thesis.

As it has already been mentioned, Active Directory will replace database system where all client data will be stored. It has both a physical and a logical structure. For purpose of this thesis, the logical structure is more important than the physical. Domains are the main part of the logical structure of the Active Directory. They can be organized in different ways, such as trees where branching can be continued further. The Domains can be explained as logical units that keep users, groups, computers, and very important organizational units (OU). These OUs may represent the starting point where branching can be done. This is because under OU different groups, users can also be stored.

The physical structure of the Active Directory supports network configuration, site links subnet objects. Sites are important in an enterprise-level multiple location network, for creating a topology that optimizes the process of replicating Active Directory information between domain controllers (DCs). They are also used for allowing process of the authentication making them more optimized.

There are a few very important components of Active Directory that should be understood before creating one. It is important to remember that AD is not only a security service for network but also a database containing configuration information about it. [17]

Active directory elements:

- Active Directory Administrative Center
- Active Directory domain controllers
- The Active Directory data store
- Active Directory partitions
- Active Directory trust relationships
- Active Directory domain name

### 7.3.1 Active Directory Administrative Center

A newer version of Windows Server (from 2008 R2) Active Directory includes Web services that provide management capabilities for Active Directory. They are mainly built to support administrators to remotely control Active Directory using PowerShell. Administrative Center (ADAC) represents surrounding where management tasks can



be managed via an easy-to-use interface built on top of PowerShell. Basically, this allows administrator to use the GUI interface to successfully achieve tasks and using GUI to send and call PowerShell script to complete the requested task.

### ■ 7.3.2 Active Directory domain controllers

The domain controllers or shorter DC represent in its core a server with the Active Directory Domain Services (DS). All DCs contain a copy of the AD database.

### ■ 7.3.3 The Active Directory data store

Each DC domain consists of a Active Directory database, that has been saved on it. The file version where database is stored is named NTDS.DIT file located in the NTDS folder of the system root. Here is used process known as multimaster replication that guarantees that the data store is consistent on all DCs. This replication allows administrators to make changes on any DC in the domain and be confident that those changes will replicate to all other DCs. [17]

### ■ 7.3.4 Active Directory partitions

There are three different partitions that are duplicated to all DCs:

- *Domain partition:* This partition contains data related to the Active Directory domain. Objects such as users, groups, computer or printers are in this partition.
- *Schema partition:* Includes the attributes and classes that make up the Active Directory schema. Attributes defines type and linking process to other Active Directory objects.
- *Configuration partition:* In this partition is comprised all information about the configuration of Active Directory.

### ■ 7.3.5 Active Directory trust relationships

This part of the Active Directory permits administrator to manage permissions to user in more than one Active Directory domain. This means that they are able to assign authorization to users or groups in a different domain. Basically, this can allow users in domain, for example nvision.com to have access to all resources that are registered to a domain under name voice.com. There are several different types of relationship trusts:

- *Forest trust:* As the name alone explains, this is a trust relationship between two different forests. It includes all domains in one forest to trust to all domains in another.
- *Shortcut trust:* This is a trust created manually between two different domains.
- *External trust:* This trust can be one-way or two-way trust. It is characteristics trust between two domains excluding the third one.
- *Realm trust:* This trust enables communication between Windows Server domain and another for example Kerberos compliant realm such as UNIX or Linux environments.

## Chapter 8

### Implementation

The most important chapter of this thesis is the implementation part. Chapter number 8 will contain realization of solution plan described in a previous part. The process of realization will be explained same as the result of the project. Step by step description will be used to illustrate each phase of the project. First part will contain explanation connected to virtual machine and different operating system. Achievement of proper set up of the web application and Microsoft Windows server containing Active Directory. After that, making secure connection and authentication process is also defined in this chapter.

#### 8.1 Project realization

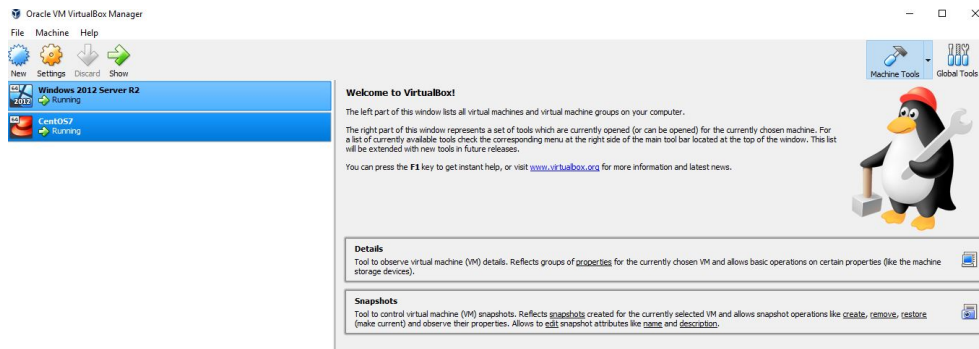
First step of the realization of this project was to make clear thoughts about which operational systems are going to be used for purpose of web application and Active Directory. After research part it has been concluded that for the web application some of the Linux system will best suit. Of course Active Directory is a part of the Microsoft Windows system so it has been concluded to use Windows 2012 Server R2 for this aim. Regarding to consultation and investigate done in first part of the project CentOS 7 was selected to be base of the web application that is going to represent EMS.

To make it easier and not to spend time and other resources on installing different operating systems it has been decided to implement Virtual Box machine for the background substrate for CentOS 7 and Microsoft Windows Server 2012 R2.

##### 8.1.1 Virtual Box Machine

VirtualBox supports large number of different (32-bit and 64-bit) operating systems. It has been considered as a “hosted” hypervisor. VirtualBox is functionally identical on all of the host platforms, which means that same file and image formats are used. Also one very important thing is that usage of this virtual machine enable running one virtual machine on host even when that machine is created on another. VirtualBox is environment that in most of cases does not require hardware virtualization. It provides to a user to be able to manage different number of unique groups feature by making it easier to control and organize. In addition to basic groups, it is also possible for any VM to be in more than one group, and for groups to be nested in a hierarchy. VirtualBox has an extremely modular design with well-defined internal programming interfaces and a clean separation of client and server code. This makes it easy to control it from several interfaces at once.

As it has been written in earlier parts, CentOS 7 and Microsoft Windows Server 2012 R2 were created by using VirtualBox platform. Installation of these two operating systems was the first step in realization of this project. Figure 8.1 shows the VirtualBox environment with successfully installed and ran systems.



**Figure 8.1.** VirtualBox environment with operating systems

### 8.1.2 CentOS 7

The CentOS 7 represents one of several Linux distribution. It has been described as a stable, easy to manage and very reproducible platform. It sources were derived out of Red Hat Enterprise Linux (RHEL). It tends to be functionally compatible with RHEL. It is no-cost and free to redistribute platform. CentOS is developed by a small team of core developers. This team is supported by an active user community, including system administrators, network administrators, manager and etc.

Because of these facts it has been decided to use this platform for running our test web application. This application was written in several java scripts files and with usage of node.js was run on CentOS. The console look of web application is shown on Figure 8.2.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-693.21.1.el7.x86_64 on an x86_64

localhost login: root
Password:
Last login: Sun May 20 13:53:56 on tty1
[root@localhost ~]# cd ..
[root@localhost /]# systemctl stop httpd
[root@localhost /]# cd var/www/html/test/
[root@localhost test]# node app
Web application - Nvision SCP Platform
```

**Figure 8.2.** CentOS 7 console look - Web Application

Part of the code that represents how the CentOS 7 server was set up and application was started:

```
// create and run HTTPS server, bind to express app
var server = require('http').createServer(app).listen(80);

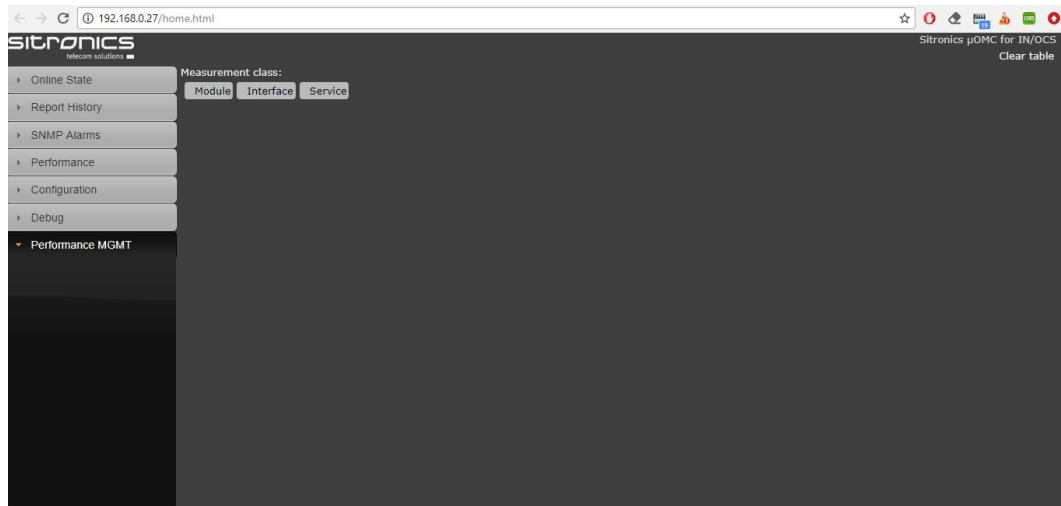
// log requests
//app.use(express.logger('dev'));

app.use(express.static(__dirname + '/public'));

app.listen(8888, function () {
  console.log('Web application - Nvision SCP Platform');
});
```

The rest of the code will be added in appendix part.

Figure 8.3 shows the look of GUI of the web application run on the CentOS server:



**Figure 8.3.** Nvision Web Application

Test application called Nvision test platform, is used as the EMS in this project. The main aim of this platform is to be used for simulation of authentication and authorization process. According to plan, it has been structured in a way that different users in different organizational units (in Active Directory) will be able to work with different modules of this application. This process will be described in LDAP part. To preform login question before user can access to this part of the application login.js together with login.html were constructed. Part of the login.js code is shown below:

```
function validate()
{
  var username = document.getElementById("username").value;
  var password = document.getElementById("password").value;
```

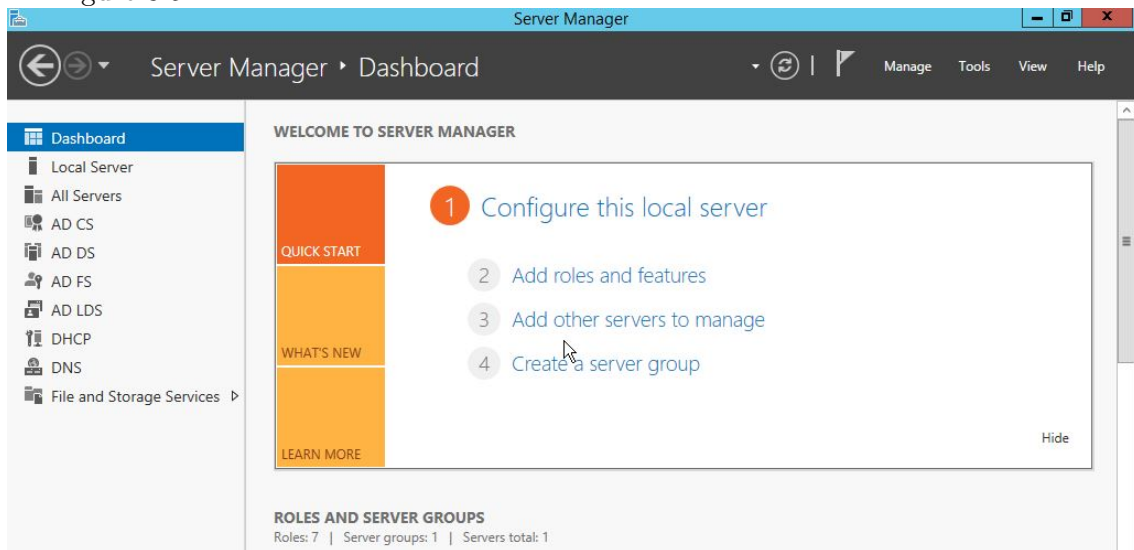
As it can be seen from the code, login.js was created in a way that from the user will be asked to input username and password for the authentication process. This part is very important because if the input credentials are not registered in Active Directory access is denied. For test purposes login window was created and it looks like:

**Figure 8.4.** Login window

In this project there is no need to explain and describe in details core of the web application and to show code lines of each module. This is because main goal of the thesis is to show authentication and authorization processes. Next subsection will explain Windows Server side, together with the organization of the Active Directory.

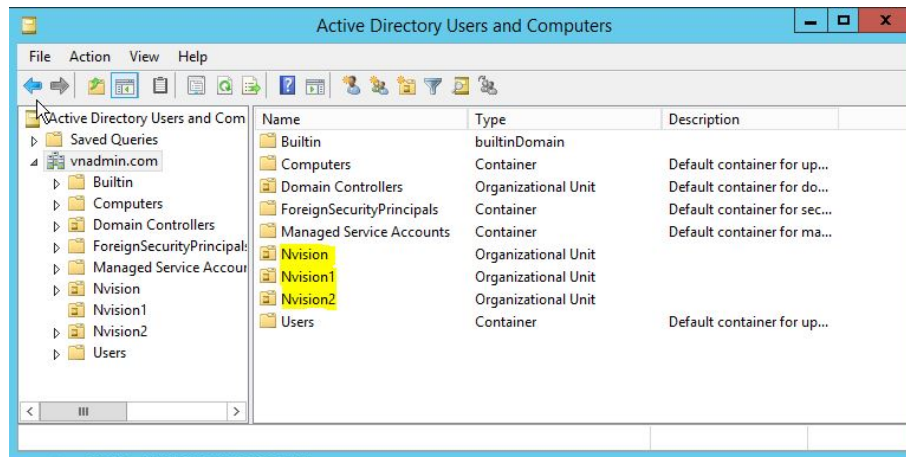
### 8.1.3 Windows Server 2012 R2 - Active Directory

After successfully installed Windows Server 2012 R2 on the VirtualBox machine, its configuration is necessary. In order to get Domain Name System (DNS) on the server installation process of DNS Server Role must be done. Also to be able to get automatically assign an IP address to the server Dynamic Host Configuration Protocol or shorter DHCP must also be installed and configured. The most important part of the server services that were installed and configured was the Active Directory service. List of the all services that were implemented on the server can be seen on Figure 8.5.



**Figure 8.5.** List of server services installed on Windows Server 2012 R2

Chapter 7 covers a detail explanation of the structure and the main part of the Active Directory service. Here only the structure of this service that will be used for the project will be described. As the Active Directory has the aim to store user's data and credentials used for authentication and authorization process it is going to contain three different Organizational Units (OU) for the test version of the process. In previous part it was explained that the idea is to disable access to some parts of the application to users that are in different OU. Users that do not belong to one of these OUs will not be able to access application at all. Figure 8.6. shows the list of three different OUs that will be used for authentication and authorization process:



**Figure 8.6.** List of the different Organizational Units that will be used in authentication process

These OUs can be named in different ways, for example if it will contain users that represents administrators in the company, it can be named as Administrators. In this case it has been named Nvision, Nvision1 and Nvision2 Organizational Unit. First OU, named Nvision will contain user with the most available system administration. This means that access to all modules of the application will be enabled to these users. Nvision1 OU will contain users with the less rights than users in previous OU. And in the last OU will be users that will have access to only one module. On this way, process of authentication and authorization of the users is going to be simulated.

#### 8.1.4 LDAP protocol

After the research part and after solution plan is created it has been decided to use LDAP protocol for the authentication and authorization process. This is decided because of many advantages that LDAP provides to both client/server sides. When it was set up that both sides can communicate between themselves LDAP was implemented. In app.js was added LDAP.js and it was configured to connect CentOS 7 application with the Windows Server 2012 R2. This connection is shown in a part of code:

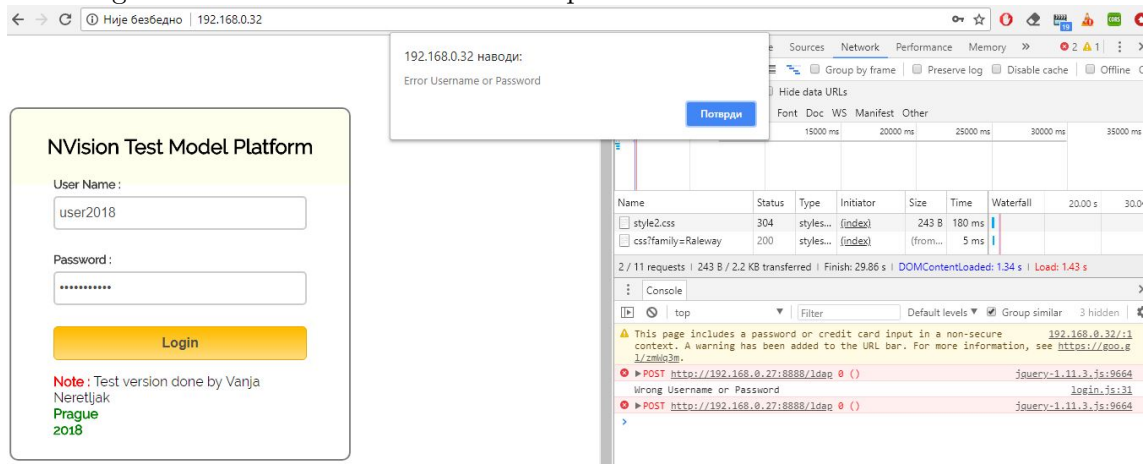
```
app.post("/ldap", function (request, response)
{
  var result = "";    // To send back to the client
  var client = ldap.createClient
  ({
    url: 'ldap://192.168.0.28'
  });
```

Once connection is established ldap bind function was created. This part of the code represents the search part where ldap search for the user in Active Directory. If the user is not found at all levels of the Active Directory access is denied.

```
client.bind(request.body.usn, request.body.psd, function(err)
{
  if (err)
  {
    //result += "Reader bind failed " + err;
    //console.log(result);
    response.send(400);
```

```
//return;
}
```

Figure 8.7 shows how the test of this part of code looks like:



**Figure 8.7.** Access denied - User does not exist in Active Directory

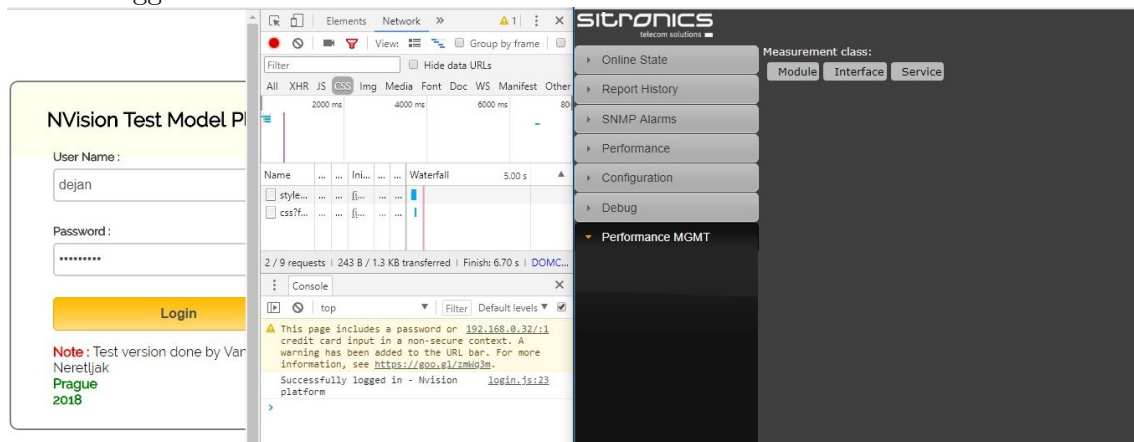
If the user that is trying to enter application is registered in Active Directory LDAP is going to check in to what OU this user belongs. The code is written in a way that if the user does not belong to the one of three already mentioned OUs access will be denied, even if the user belongs to another OU or is registered in user group of the Active Directory. Here only the first search part that LDAP is processing while trying to find user will be shown:

```
var opts =
{
    filter: '(objectClass=*)',
    scope: 'sub',
    attributes: ['dn', 'cn', 'dc', 'sn' ]
};
var notFound=true;
client.search('cn=' + request.body.usn + ',
ou=Nvision,dc=vnadmin,dc=com', opts, function(err, res)
{
    //console.log(res);
    res.on('searchEntry', function(entry)
    {
        console.log('Welcome to Nvision SCP Platform - '
+ request.body.usn + ' - ADMIN');
        //console.log('entry: ' + JSON.stringify(entry.object));
        notFound = false;
        response.send(200);
    });
});
```

At the beginning of the code it has been determined in what way search will be done. Filter, scope and attributes define search options. After it is stated where the search will start. Username is used for the finding of a user. In this case search will start in first OU – Nvision. If the user is found in this OU application will be directed to the home.html where the user will be able to see all modules. In case that user is not found in this OU the search continues to second and if the same case happens in second, search will continue to the third and last OU. Figure 8.8 shows the process of



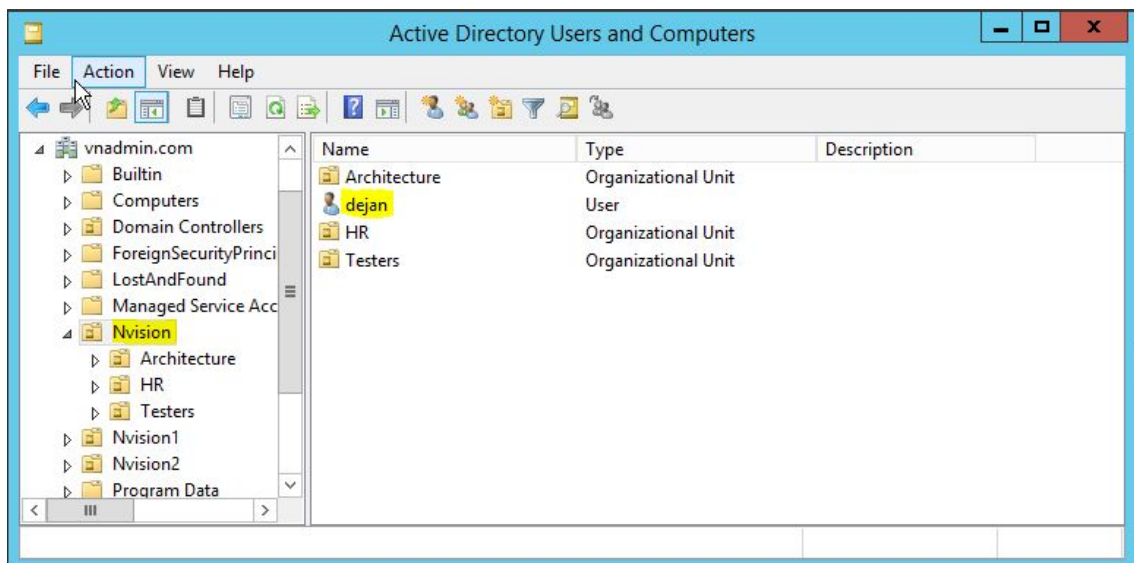
successfully done authentication and authorization rights. In this case user registered under the OU – Nvision (the OU with the highest authorization rights) successfully was logged in.



**Figure 8.8.** Successfully login operation - Administrator group

The Figure 8.9 shows the user registered with credentials:

- Username: dejan
- Password: Nedic1992



**Figure 8.9.** Registered user in Active Directory

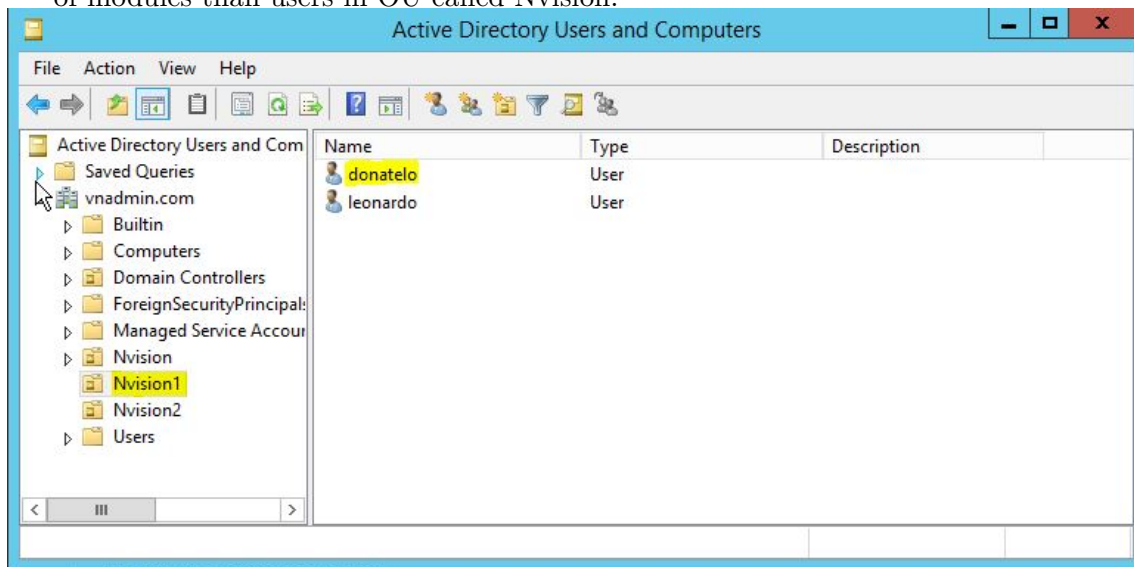
This was first successfully attempted authentication and authorization process. Next two test cases show situation where user is registered in Organizational Units named Nvision1 and Nvision2.

### 8.1.5 Test Case - Nvision1

In order to make successful implementation of the system in real world project, it is very important to examine all possible test cases that can occur. In previous part it has been shown two different situations where user access is denied and situation where user has access to all modules of the platform. According to topic of the thesis, it is necessary to do at least few more test cases. In subsection 8.1.5 will be presented situation where user is registered in Organizational Unit named Nvision1. This OU



contains users that belongs to Architects group. These users can access less number of modules than users in OU called Nvision.

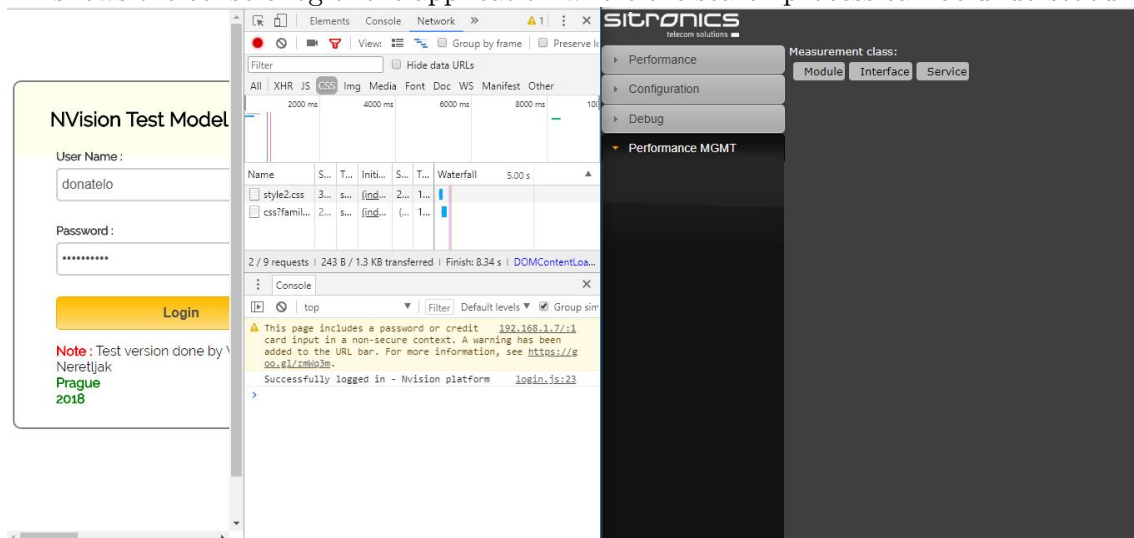


**Figure 8.10.** Registered user in Active Directory - OU Nvision1

Figure 8.10 shows a user that is registered in Active Directory OU named Nvision1. Credentials of this user are:

- Username: donatelo
- Password: Crvena2018

Login process is presented on next Figure 8.11. As it can be seen from the part where the web application is revealed this user have limited access to it. Figure 8.12 shows the console log of the application where the search process can be understood.



**Figure 8.11.** Successfully login operation - Architect group

```
Web application - Nvision SCP Platform
User donatelo does not belong to ADMIN Group
Welcome to Nvision SCP Platform - donatelo - ARCHITECT
```

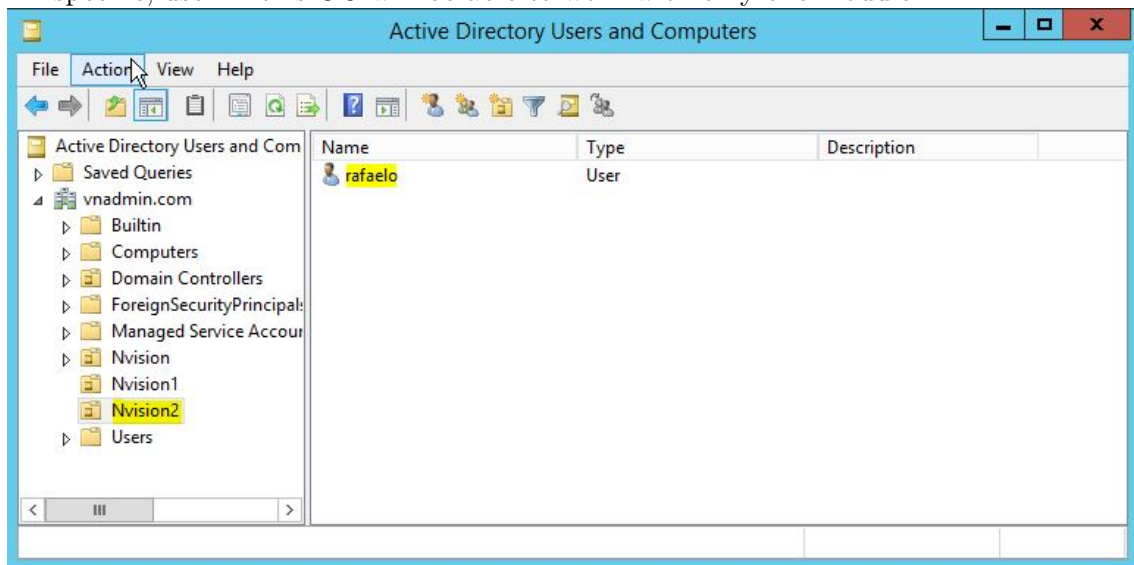
**Figure 8.12.** Console search status

This test case showed process of authentication and authorization of the user that is registered in OU named Nvision1. To this Organizational Unit were added

limitation that are not connected with the first OU. User that belongs to this part of Active Directory is able to see and use few modules less. This way different way of authentication and authorization has been represented. The next test case will illustrate situation where user belongs to the third and last OU – Nvision2.

### 8.1.6 Test Case - Nvision2

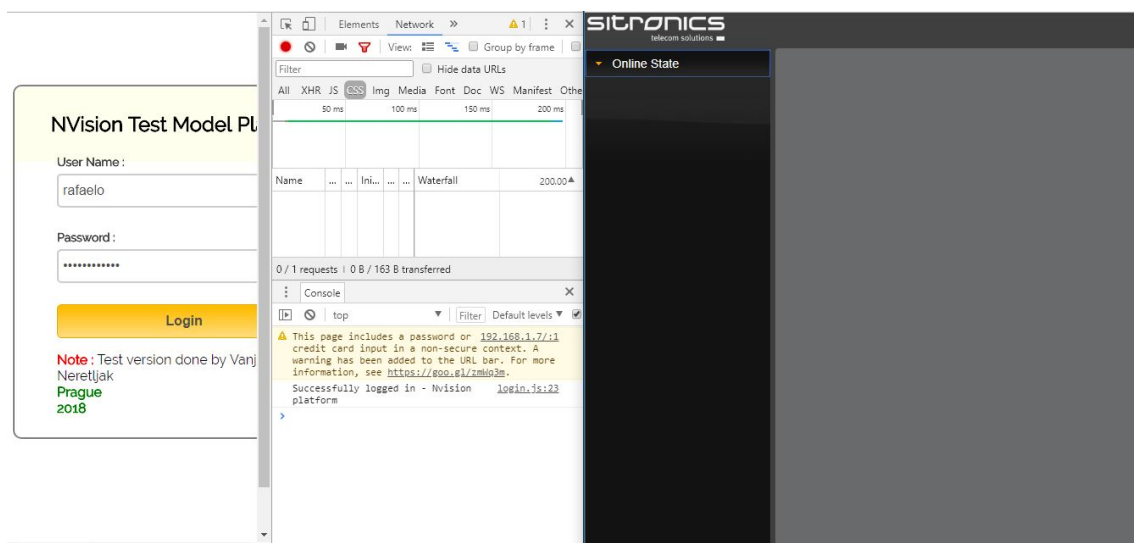
As it was mentioned in earlier subsection in this part the last test case will be described. This test is connected with third Organizational Unit named Nvision2. In this OU, user belongs to so-called Tester Group. This means that this OU has the lowest number of enabled modules in web application. To be more precise and specific, user in this OU will be able to work with only one module.



**Figure 8.13.** Registered user in Active Directory - OU Nvision2

Login process is presented on Figure 8.14 together with next Figure 8.15 that shows the console search procedure. This user is registered under credentials:

- Username: rafaelo
- Password: Scemlija2018



**Figure 8.14.** Successfully login operation - Tester group



```
Web application - Nvision SCP Platform
User rafaelo does not belong to ADMIN Group
User rafaelo does not belong to a ARCHITECT Group
Welcome to Nvision SCP Platform - rafaelo - TESTER
```

**Figure 8.15.** Console search status

The last prepared test case was successfully completed. These test cases show some of the possibilities that can occur in the process of authentication and authorization of users. Active Directory enables very easy managing of user accounts and redirecting them to different levels of authorization rights.

## Chapter 9

### Conslusion

At the very beginning, the main goal of this thesis was set up. Successful process of authentication and authorization process in modern telecommunication systems was established. Using LDAP protocol, it has been positively set up connection between Active Directory on one side and web application on another. Different users gain limited access to different modules. According to architectural plan, process should work in a way to check presence of the user credentials in Active Directory, and according to an Organizational Unit to give him/her authorization rights.

Usage of the test platform in a shape of web application gave us possibility to successfully manage all test cases. Not only positive tests such is successful login of a user that is registered in one of three OUs, but also so-called negative test cases where user access to web application is denied. Existing limitations are taken to the minimum level so this project can be used in practical work.

The idea of this thesis led us to a project that, even similar ways of authentication and authorization already exists, can be implemented for a purpose of telecommunication company named Nvision, a.s. The objective of the thesis was to make process that will be used in company software architecture and with configuration set up this is possible. Also this system is made to be very easy changed and improved at all levels.

### 9.1 Future work

At this level project can be used, but of course there is always space for implementation of new items. Firstly, in the future work the security system should be improved on a higher level. The best way for this to be done is to implement LDAPS system. LDAP traffic can be much more confidential and secure by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) technology. This can be done by installing a properly formatted certificate that will enable LDAP over SSL. Also configuration of Active Directory can be moderated and improved in a way of adding and putting users into different groups. In a case where one user belongs to more groups it can be done to send a question to a user where system will ask under what credentials and rights he/she wants to login. In a current system this is done to open the application and give a user the rights that belongs to the highest Organizational Unit. By implementing this system to a real-world system further development direction can be decided upon.

## References

- [1] Quang-Dung Ho, Daniel Tweed, and Tho Le-Ngoc. *LTE-Advanced: An Overview*. Springer International Publishing, Cham, 2017.  
[https://doi.org/10.1007/978-3-319-47346-8\\_3](https://doi.org/10.1007/978-3-319-47346-8_3).
- [2] Thomas Derham. Chapter 9 - lte and lte-advanced. In Alain Sibille, Claude Oestges, and Alberto Zanella, editors, *MIMO*, pages 243 – 265. Academic Press, Oxford, 2011.  
<https://www.sciencedirect.com/science/article/pii/B9780123821942000095>.
- [3] Fikadu B. Degefa, Donghoon Lee, Jiye Kim, Younsung Choi, and Dongho Won. Performance and security enhanced authentication and key agreement protocol for sae/lte network. *Computer Networks*, 94:145 – 163, 2016.  
<http://www.sciencedirect.com/science/article/pii/S1389128615004211>.
- [4] A. Gupta and R. K. Jha. A survey of 5g network: Architecture and emerging technologies. *IEEE Access*, 3:1206–1232, 2015.
- [5] Kuppusamy Peramandai Govindasamy. A comparative study on 4g and 5g technology for wireless applications. 01 2015.
- [6] G. Reali and L. Monacelli. Definition and performance evaluation of a fault localization technique for an ngn ims network. *IEEE Transactions on Network and Service Management*, 6(2):122–136, June 2009.
- [7] Toni Janevski. *Index*, pages 368–. Wiley Telecom, 2014.  
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=8043871>.
- [8] N. Ahmed and C. D. Jensen. Definition of entity authentication. In *2010 2nd International Workshop on Security and Communication Networks (IWSCN)*, pages 1–7, May 2010.
- [9] E. Schiavone, A. Ceccarelli, and A. Bondavalli. Continuous authentication and non-repudiation for the security of critical systems. In *2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS)*, pages 207–208, Sept 2016.
- [10] Jonathon E. Tidswell and John M. Potter. A graphical definition of authorization schema in the dtac model. In *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*, SACMAT '01, pages 109–120, New York, NY, USA, 2001. ACM.  
<http://doi.acm.org/10.1145/373256.373276>.
- [11] Confidentiality, integrity, availability: The three components of the cia triad.  
<https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/>.
- [12] J. Kohl and C. Neuman. The kerberos network authentication service (v5), Jan 1993.  
<https://www.rfc-editor.org/info/rfc1510>.
- [13] Steven Tuttle. *Understanding LDAP design and implementation*. IBM, International Technical Support Organization, 2004.

- [14] Tim howes interview, part 2: Securing decentralized it, Aug 2017.
- [15] Chapter 5 - communication security: Web based services. In Ido Dubrawsky, editor, *How to Cheat at Securing Your Network*, How to Cheat, pages 165 – 236. Syngress, Burlington, 2007.  
<https://www.sciencedirect.com/science/article/pii/B9781597492317500083>.
- [16] F. Nie, F. Xu, and R. Qi. Saml-based single sign-on for legacy system. In *2012 IEEE International Conference on Automation and Logistics*, pages 470–473, Aug 2012.
- [17] Tony Redmond. 2 - exchange, windows, and the active directory. In Tony Redmond, editor, *Microsoft Exchange 2007*, HP Technologies, pages 47 – 98. Digital Press, Burlington, 2007.  
<https://www.sciencedirect.com/science/article/pii/B978155558347750003X>.